HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

| Tiedekunta/Osasto Fakultet/Sektion – Faculty<br>Matemaattis-luonnontieteellinen tiedekunta | Laitos/Institution– Department<br>Matematiikan ja tilastotieteen laitos | |
|---|---|---|
| Tekijä/Författare – Author<br>Anna-Mari Pulkkinen | | |
| Työn nimi / Arbetets titel – Title<br>Kertalukua 1-15 olevat ryhmät | | |
| Oppiaine /Läroämne – Subject<br>Matematiikka | | |
| Työn laji/Arbetets art – Level<br>Pro Gradu -tutkielma | Aika/Datum – Month and year<br>Huhtikuu 2014 | Sivumäärä/ Sidoantal – Number of pages<br>44 s |

Tiivistelmä/Referat – Abstract

Ryhmäteorian eräänä päämääränä voidaan pitää äärellisten ryhmien löytämistä. Tässä tutkielmassa esittelen kaikki ryhmät aina kertalukuun 15 asti. Lisäksi osoitan, ettei muita korkeintaan kertalukua 15 olevia ryhmiä ole mahdollista löytyä. Algebran näkökulmasta ryhmät ovat samoja, jos niissä on täsmälleen samanlainen rakenne, vaikka niissä olisikin eri alkiot. Tällöin sanotaan, että ryhmät ovat isomorfisia keskenään.

Tutkielman sisältö voidaan jakaa kahteen osaan. Ensimmäisessä osassa esittelen algebran keskeisimmät käsitteet, joitain esimerkkejä sekä hyödyllisiä lauseita ja korollaareja. Määränpääni saavuttamisen kannalta merkittävimmät lauseet, Lagrangen lauseen ja Sylowin lauseet, olen esittänyt omissa luvuissaan. Lagrangen lauseen mukaan aliryhmän kertaluku jakaa ryhmän kertaluvun. Toisaalta tästä seuraa, että myös ryhmän alkion kertaluku jakaa ryhmän kertaluvun. Tämän lauseen avulla voidaan päätellä, millaisia alkioita ryhmät voivat sisältää. Sylowin lauseet puolestaan kertovat millaisia aliryhmiä ryhmät sisältävät. Peter Sylow osoitti, että jokaista ryhmän kertaluvun tekijää kohti, joka on jokin alkuluvun potenssi, löytyy aliryhmä, jonka kertaluku on tämä alkuluvun potenssi. Sylowin lauseiden avulla voidaan päätellä esimerkiksi näiden aliryhmien lukumääriä. Diedriryhmät olen käsitellyt omassa luvussa, jossa esittelen myös symmetrisen ryhmän käsitteen.

Tutkielman toinen puolisko keskittyy korkeintaan kertalukua 15 olevien ryhmien löytämiseen. Samalla tavalla käyttäytyvät kertaluvut on käsitelty samassa luvussa. Esimerkiksi kaikki ryhmät, joiden kertaluku on jokin alkuluku, ovat syklisiä eli yhden alkionsa virittämiä. Ryhmät joiden kertaluku on jonkin alkuluvun toinen potenssi käyttäytyvät keskenään samoin, kuten myös ryhmät, joiden kertaluku on $2p$, kun $p$ on jokin lukua kaksi suurempi alkuluku. Vaihdannaiset eli Abelin ryhmät voidaan löytää kaikkien kertalukujen tapauksessa helposti tutkielman ensimmäisessä osassa esittelemieni tulosten avulla. Epävaihdannaisten ryhmien tarkastelu on huomattavasti monimutkaisempaa. Tällaisten ryhmien aliryhmille ja alkioille voidaan löytää joitain ehtoja esimerkiksi Lagrangen lauseen ja Sylowien lauseiden avulla. Näin päästään usein käsiksi ryhmän virittäjäalkioihin ja sitä kautta johonkin konkreettiseen ryhmään. Tutkielman viimeisessä luvussa on vielä koottuna taulukkoon kaikki korkeintaan kertalukua 15 olevat ryhmät.

Avainsanat – Nyckelord – Keywords
algebra, ryhmäteoria, ryhmä, diedriryhmä, Lagrangen lause, Sylowin lauseet

Säilytyspaikka – Förvaringställe – Where deposited
Kumpulan tiedekirjasto

Muita tietoja – Övriga uppgifter – Additional information

# Kertalukua 1–15 olevat ryhmät

Anna-Mari Pulkkinen

28.4.2014

# Sisältö

# Luku 1

# Johdanto

Ryhmäteorian synnyn ajankohtaa on vaikea määritellä, mutta tiettävästi ensimmäisen kerran käsitettä *ryhmä* käytti ranskalainen matemaatikko Évariste Galois 1830-luvulla. Nykyisin tunnetun muotonsa ryhmän määritelmä saavutti tosin vasta 1900-luvulla ([3], s. 34). Toisaalta ennen kuin ryhmäteoriasta edes puhuttiin, niin muun muassa Joseph-Louis Lagrange esitti päätelmiä ([3], s. 128), jotka esittelen myös tässä Pro Gradu -tutkielmassani.

Algebran keskiössä olevan ryhmäteorian maalina voidaan pitää kaikkien ryhmien löytämistä. Tutkielmani tarkoituksena on löytää ja esitellä kaikki ryhmät, joissa on korkeintaan 15 alkiota. Algebran näkökulmasta ryhmät ovat samoja, jos niissä on täsmälleen samanlainen rakenne, vaikka niissä olisikin eri alkiot. Tällöin sanotaan, että ryhmät ovat isomorfisia keskenään.

Ensimmäisessä luvussa esittelen tärkeimmät algebralliset määritelmät ja muita tuloksia, jotka ovat tutkielmani myöhemmässä vaiheessa hyödyksi. Toisessa ja kolmannessa luvussa perehdyn eräisiin ryhmäteorian merkittävimpiin lauseisiin: Lagrangen lauseeseen ja Sylowin lauseisiin. Nämä lauseet ja niihin liittyvät korollaarit ovat suureksi avuksi tutkielman myöhemmissä luvuissa. Tutkielmani neljäs luku käsittelee symmetrisiä ryhmiä sekä diedriryhmiä.

Viisi ensimmäistä lukua ovat siis johdattelua Pro Gradu -tutkielmani varsinaisen määränpään saavuttamiseksi. Löytääkseni kaikki korkeintaan kertalukua 15 olevat ryhmät esittelen nämä ryhmät ja niiden alkiot, sekä osoitan, ettei algebran näkökulmasta muita ryhmiä ole mahdollista löytää. Samoin käyttäytyvät kertaluvut olen sijoittanut samaan lukuun. Esimerkiksi ryhmät, joiden kertaluku on jokin alkuluku käsitellään yhdessä luvussa ja ryhmät, joiden kertaluku on jonkin alkuluvun toinen potenssi käsitellään omassa luvussaan. Viimeisessä luvussa olen koonnut yhteen taulukkoon kaikki ryhmät, joiden kertaluku on korkeintaan 15.

# Luku 2

# Ryhmien ominaisuuksia

Tässä luvussa esittelen Pro Gradu -tutkielmani kannalta tärkeät algebralliset käsitteet ja niihin liittyvät lauseet. Merkinnöissä noudatan Jokke Häsän ja Johanna Rämön Algebra I -kurssin oppikirjan *Johdatus abstraktiin algebraan* merkintöjä sekä Jokke Häsän luentomateriaalia *Algebra II* (Matematiikan ja tilastotieteen laitos, kevät 2010, Helsingin yliopisto.)

**Määritelmä 2.1.** Olkoon $G$ epätyhjä joukko varustettuna laskutoimituksella, joka liittää jokaiseen joukon $G$ alkiopariin $(a, b)$ jonkin kolmannen alkion $c$ joukosta $G$. Sanotaan, että $G$ on *ryhmä*, jos seuraavat ehdot toteutuvat:

**(G1)** Laskutoimitus on liitännäinen eli $(ab)c = a(bc)$ $\forall a, b, c \in G$.

**(G2)** Joukossa $G$ on neutraalialkio $e$, siten että $ae = ea = a$ $\forall a \in G$.

**(G3)** Jokaisella alkiolla $a \in G$ on käänteisalkio $b \in G$, siten että $ab = ba = e$.

Jos lisäksi ryhmälle $G$ pätee $ab = ba$ $\forall a, b \in G$, niin kyseessä on vaihdannainen ryhmä eli *Abelin ryhmä*.

**Määritelmä 2.2.** Jos ryhmän $G$ osajoukko $H$ on itsekin ryhmä varustettuna ryhmän $G$ laskutoimituksella, niin sanotaan, että $H$ on ryhmän $G$ *aliryhmä* ja merkitään $H \leq G$. Tämän osoittamiseksi riittää osoittaa, että seuraavat ehdot pätevät:

**(H1)** Joukko $H$ on suljettu laskutoimituksen suhteen eli jos $g, h \in H$, niin $gh \in H$.

**(H2)** Ryhmän $G$ neutraalialkio on joukossa $H$.

**(H3)** Joukko $H$ sisältää kaikkien alkioidensa käänteisalkiot eli jos $g \in H$, niin $g^{-1} \in H$.

**Lause 2.3.** *Olkoon $H$ ryhmän $G$ epätyhjä osajoukko. Tällöin $H$ on ryhmän $G$ aliryhmä, jos ja vain jos*

$$ab^{-1} \in H \quad \text{kaikilla} \quad a, b \in H.$$

*Todistus.* Jos $H$ on aliryhmä ja $a, b \in H$, niin myös $ab^{-1} \in H$. Lisäksi aliryhmä on aina epätyhjä, koska se sisältää neutraalialkion. Oletetaan seuraavaksi, että $H$ on ryhmän $G$ epätyhjä osajoukko ja $ab^{-1} \in H$ kaikilla $a, b \in H$. Osoitetaan, että tällöin $H \leq G$. Käydään läpi kohdat (H1)–(H3):

**(H2)** Koska $H$ on epätyhjä, niin on olemassa jokin $a \in H$. Oletuksen nojalla $e = aa^{-1} \in H$.

**(H3)** Olkoon $b \in H$. Edellisen kohdan perusteella $e \in H$. Tällöin oletuksesta seuraa $b^{-1} = eb^{-1} \in H$.

**(H1)** Oletetaan, että $a, b \in H$. Edellisestä kohdasta seuraa, että $b^{-1} \in H$, jolloin $ab = a(b^{-1})^{-1} \in H$, joten $H$ on suljettu laskutoimituksen suhteen.

Nyt on osoitettu, että $H \leq G$. □

**Esimerkki 2.4.** Määritellään joukkojen $H$ ja $K$ karteesinen tulo $H \times K$ joukkona, joka sisältää kaikki parit $h, k$, jossa ensimmäinen koordinaatti $h \in H$ ja jälkimmäinen $k \in K$. Jos $H$ ja $K$ ovat ryhmiä, niin voidaan määritellä joukon $H \times K$ alkioille tulo seuraavasti. Olkoot $(h_1, k_1), (h_2, k_2) \in H \times K$ ja määritellään

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2),$$

missä $h_1 h_2$ ja $k_1 k_2$ ovat ryhmissä $H$ ja $K$ määritellyt tulot. Osoitetaan, että $H \times K$ on ryhmä tällä laskutoimituksella määriteltynä. Huomataan ensiksi, että $H \times K$ on selvästi suljettu tämän tulon suhteen. Käydään läpi ryhmäaksioomat, jotka seuraavat ryhmien $H$ ja $K$ ominaisuuksista.

**(G1)** Olkoot $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$. Tällöin

$$\begin{aligned}
[(h_1, k_1) \cdot (h_2, k_2)] \cdot (h_3, k_3) &= (h_1 h_2, k_1 k_2) \cdot (h_3, k_3) \\
&= ((h_1 h_2) h_3, (k_1 k_2) k_3) \\
&= (h_1 (h_2 h_3), k_1 (k_2 k_3)) \\
&= (h_1, k_1) \cdot (h_2 h_3, k_2 k_3) \\
&= (h_1, k_1) \cdot [(h_2, k_2) \cdot (h_3, k_3)].
\end{aligned}$$

Laskutoimitus on siis liitännäinen joukossa $H \times K$.

**(G2)** Olkoon ryhmän $H$ neutraalialkio $e$ ja ryhmän $K$ neutraalialkio $e'$ ja olkoon lisäksi $(h,k) \in H \times K$. Nyt

$$(e,e') \cdot (h,k) = (eh, e'k) = (h,k) = (he, ke') = (h,k) \cdot (e,e'),$$

joten alkio $(e,e')$ on joukon $H \times K$ neutraalialkio.

**(G3)** Jos $(h,k) \in H \times K$, niin $(h^{-1}, k^{-1})$ on sen käänteisalkio, sillä

$$(h,k) \cdot (h^{-1}, k^{-1}) = (hh^{-1}, kk^{-1}) = (e,e') = (h^{-1}h, k^{-1}k) = (h^{-1}, k^{-1}) \cdot (h,k).$$

Tällaista ryhmää $H \times K$ kutsutaan ryhmien $H$ ja $K$ *suoraksi tuloksi*.

**Määritelmä 2.5.** Ryhmän alkioiden lukumäärää kutsutaan *ryhmän kertaluvuksi*. Ryhmän $G$ kertaluku merkitään $|G|$.

**Määritelmä 2.6.** *Alkion $g$ kertaluku* ryhmässä $G$ on pienin positiivinen kokonaisluku $n$, jolla pätee $g^n = e$. Tällöin merkitään $|g| = n$. Jos tällaista kokonaislukua $n$ ei löydy, niin sanotaan, että alkion $g$ kertaluku on ääretön.

**Määritelmä 2.7.** Olkoon $G$ ryhmä ja $S$ sen osajoukko. Tällöin joukon $S$ *virittämä* aliryhmä $\langle S \rangle$ on pienin ryhmän $G$ aliryhmä, joka sisältää joukon $S$.

**Määritelmä 2.8.** Ryhmää $G$ sanotaan *sykliseksi*, jos se on yhden alkionsa virittämä, eli $G = \langle g \rangle$ jollakin $g \in G$.

**Määritelmä 2.9.** Olkoon $n$ positiivinen kokonaisluku. Kokonaisluvun $a$ *jäännösluokka modulo $n$* on joukko

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

Lukua $a$ nimitetään jäännösluokan $[a]_n$ *edustajaksi*.

**Esimerkki 2.10.** Jäännösluokkien joukoksi modulo $n$ kutsutaan joukkoa

$$Z_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

jossa $n \in \mathbb{Z}$. Näytetään, että tämä joukko yhteenlaskulla varustettuna on ryhmä. Ensin on varmistettava, että jäännösluokkien joukossa voidaan määritellä yhteenlasku

$$[a]_n + [b]_n = [a+b]_n.$$

Yhteenlaskun tulokseen ei saa siis vaikuttaa edustajan valinta. Olkoot $[a]_n = [a']_n$ ja $[b]_n = [b']_n$. Tällöin määritelmän mukaan $a \equiv a' \pmod{n}$ ja $b \equiv b' \pmod{n}$. Kongruenssien laskusäännöt oletetaan tässä tutkielmassa tunnetuksi, jolloin $a+b \equiv a'+b' \pmod{n}$. Siis $[a+b]_n = [a'+b']_n$ ja jäännösluokkien yhteenlasku on hyvin määritelty. Huomataan lisäksi, että $\mathbb{Z}_n$ on suljettu yhteenlaskun suhteen, sillä jos $[a]_n, [b]_n \in \mathbb{Z}_n$, niin $[a]_n + [b]_n = [a+b]_n \in \mathbb{Z}_n$. Ryhmäaksioomat seuraavat suoraan kokonaislukujen yhteenlaskun ominaisuuksista:

**(G1)** Olkoot $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$. Tällöin

$$\begin{aligned}([a]_n + [b]_n) + [c]_n &= [a+b]_n + [c]_n \\ &= [(a+b)+c]_n \\ &= [a+(b+c)]_n \\ &= [a]_n + [b+c]_n \\ &= [a]_n + ([b]_n + [c]_n)\end{aligned}$$

eli laskutoimitus on liitännäinen.

**(G2)** Neutraalialkio on $[0]_n$, sillä

$$[0]_n + [a]_n = [0+a]_n = [a]_n = [a+0]_n = [a]_n + [0]_n$$

kaikilla $[a]_n \in \mathbb{Z}_n$.

**(G3)** Alkion $[a]_n \in \mathbb{Z}_n$ vasta-alkio on $[-a]_n$, sillä

$$[a]_n + [-a]_n = [a-a]_n = [0]_n \text{ ja } [-a]_n + [a]_n = [-a+a]_n = [0]_n.$$

Jäännösluokkien joukko $\mathbb{Z}_n$ on siis ryhmä. Kyseessä on itse asiassa syklinen ryhmä, sillä alkio $[a]_n \in \mathbb{Z}_n$ voidaan kirjoittaa muodossa

$$[a]_n = \underbrace{[1]_n + [1]_n + \ldots + [1]_n}_{a \text{ kpl}}.$$

Alkio $[1]_n$ virittää siis ryhmän $\mathbb{Z}_n$. Joukko $\mathbb{Z}_n$ koostuu jäännösluokista $[0]_n, \ldots [n-1]_n$, joita on $n$ kappaletta. Näin ollen ryhmä $\mathbb{Z}_n$ on syklinen ja sen kertaluku on $n$.

**Lause 2.11.** *Sykliset ryhmät ovat vaihdannaisia.*

*Todistus.* Olkoon $G$ syklinen ryhmä. Oletetaan, että ryhmän $G$ alkio $g$ virittää koko ryhmän eli $G = \langle g \rangle$. Tällöin $G = \{g^0, g, g^2, \ldots\}$. Jos $a, b \in G$, niin

$$ab = g^s g^t = g^{s+t} = g^{t+s} = g^t g^s,$$

joillakin $s, t \in \mathbb{N}$. Ryhmä $G$ on siis vaihdannainen. □

**Määritelmä 2.12.** Olkoot $G$ ja $H$ ryhmiä. Kuvaus $f : G \to H$ on *homomorfismi* jos kaikilla $a, b \in G$ pätee $f(ab) = f(a) \cdot f(b)$. Jos kuvaus on lisäksi bijektiivinen, niin sen sanotaan olevan *isomorfismi* ja ryhmät $G$ ja $H$ ovat isomorfiset. Tällöin merkitään $G \cong H$ ja algebran näkökulmasta nämä ryhmät ovat samat.

**Lause 2.13.** *Olkoon $f : G \to H$ ryhmähomomorfismi. Tällöin* $\mathrm{Im}f \leq H$.

*Todistus.* Käytetään todistuksessa lausetta 2.21. Määritelmän mukaan kuvajoukko $\mathrm{Im}f$ on ryhmän $H$ osajoukko. Koska $f$ on homomorfismi, niin $f(e) = f(e \cdot e) = f(e) \cdot f(e)$. Kertomalla yhtälön molemmat puolet alkion $f(e)$ käänteisalkiolla ryhmässä $H$ saadaan $e = f(e)$. Siispä $e \in \mathrm{Im}f$, joten kuvajoukko $\mathrm{Im}f$ on epätyhjä. Oletetaan, että $a, b \in \mathrm{Im}f$, jolloin kuvajoukon määritelmän mukaan on olemassa sellaiset $x, y \in G$, että $f(x) = a$ ja $f(y) = b$. Koska $f$ on homomorfismi, niin $f(y^{-1})$ on alkion $f(y)$ käänteisalkio, sillä

$$f(y)f(y^{-1}) = f(yy^{-1}) = f(e) = e \quad \text{ja} \quad f(y^{-1})f(y) = f(y^{-1}y)f(e) = e.$$

Nyt

$$ab^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}).$$

Koska $xy^{-1} \in G$, niin $ab^{-1} = f(xy^{-1}) \in \mathrm{Im}f$ ja aliryhmäkriteerin nojalla $\mathrm{Im}f$ on ryhmän $H$ aliryhmä. □

**Lause 2.14.** *Olkoot $G$ ja $H$ ryhmiä ja olkoon $f : G \to H$ homomorfismi. Kuvaus $f$ on injektiivinen jos ja vain jos* $\mathrm{Ker}f = \{e\}$.

*Todistus.* Jos $f$ on injektio ja $a \in \mathrm{Ker}f$, niin $f(a) = e = f(e)$, joten $a = e$ ja $\mathrm{Ker}f = \{e\}$. Oletetaan seuraavaksi, että $\mathrm{Ker}f = \{e\}$. Jos $f(a) = f(b)$, niin $e = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Koska $ab^{-1} \in \mathrm{Ker}f$, niin oletuksesta seuraa, että $ab^{-1} = e$ eli $a = b$, joten kuvaus $f$ on injektio. □

**Lause 2.15.** *Jokainen äärellinen syklinen ryhmä, jonka kertaluku on $n$, on isomorfinen ryhmän $\mathbb{Z}_n$ kanssa.*

*Todistus.* Olkoon $G = \langle g \rangle$ syklinen ryhmä, jonka kertaluku on $n$. Tällöin

$$G = \{e, g^1, g^2, \ldots, g^{n-1}\}$$

ja kaikki tässä esiintyvät alkion $g$ potenssit poikkeavat toisistaan. Osoittaaksemme, että $G \cong \mathbb{Z}_n$ tarvitsee osoittaa, että näiden joukkojen välille voidaan esittää kuvaus, joka on bijektiivinen homomorfismi. Määritellään kuvaus $f : \mathbb{Z}_n \to G$ ehdolla

$$f([k]_n) = g^k.$$

Koska ehto on määritelty käyttäen sivuluokan edustajaa, täytyy varmistaa, että edustajan valinta ei vaikuta kuvauksen arvoon.

Oletetaan, että $[k]_n = [m]_n$. Nyt $k = m + an$ jollakin $a \in \mathbb{Z}$. Koska alkion $g$ kertaluku on $n$, niin

$$g^k = g^{m+an} = g^m g^{an} = g^m (g^n)^a = g^m e^a = g^m.$$

Sivuluokan edustajan valinta ei siis vaikuta ja kuvaus on näin ollen hyvin määritelty.

Huomataan, että

$$f([k]_n + [m]_n) = f([k+m]_n) = g^{k+m} = g^k g^m = f([k]_n) f([m]_n)$$

kaikilla $k, m \in \mathbb{Z}$, joten kuvaus on homomorfismi.

Oletetaan, että $f([k]_n) = f([m]_n)$ joillakin $[k]_n, [m]_n \in \mathbb{Z}_n$. Tällöin $g^k = g^m$ eli $g^{k-m} = g^0 = e$. Koska alkion $g$ kertaluku on $n$, niin luku $k - m$ on jokin luvun $n$ monikerta. Toisin sanoen $n$ jakaa luvun $k - m$ eli $k \equiv m \pmod{n}$, mikä tarkoittaa, että $[k]_n = [m]_n$. Kuvaus $f$ on siis injektio. Lisäksi jokainen ryhmän $G$ alkio on muotoa $g^k$, jollakin $k \in \{0, 1, \ldots, n-1\}$, joten kuvaus on myös surjektio. Kuvaus $f : \mathbb{Z}_n \to G$ on siis bijektiivinen. Näin ollen ryhmät $G$ ja $\mathbb{Z}_n$ ovat isomorfiset. □

**Lause 2.16.** *Olkoot $\mathbb{Z}_n$ ja $\mathbb{Z}_m$ syklisiä ryhmiä siten että $|\mathbb{Z}_n| = n$ ja $|\mathbb{Z}_m| = m$ ja* $\text{syt}(n, m) = 1$. *Tällöin $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, missä $\mathbb{Z}_{nm}$ on kertalukua $nm$ oleva syklinen ryhmä.*

*Todistus.* Lauseen 2.15 perusteella riittää osoittaa, että ryhmä $\mathbb{Z}_n \times \mathbb{Z}_m$ on syklinen ja sen kertaluku on $nm$. Olkoot $\mathbb{Z}_n = \langle g \rangle$ ja $\mathbb{Z}_m = \langle h \rangle$. Selvitetään ryhmän $\mathbb{Z}_n \times \mathbb{Z}_m$ alkion $(g, h)$ kertaluku. Jos $(g, h)^k = e$ jollakin $k \in \mathbb{Z}$, niin $(g^k, h^k) = e$ eli $g^k = e$ ja $h^k = e$. Koska $|g| = n$ ja $|h| = m$, niin $n \mid k$ ja $m \mid k$. Koska $\text{syt}(n, m) = 1$, niin luku $k$ on jaollinen luvulla $nm$. Toisaalta $(g, h)^{nm} = (g^{nm}, h^{nm}) = e$, joten alkion $(g, h)$ kertaluku on $nm$ ja $\mathbb{Z}_n \times \mathbb{Z}_m = \langle (g, h) \rangle$ eli $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$. □

**Lause 2.17.** *Jokainen äärellinen Abelin ryhmä $G$ on isomorfinen syklisten ryhmien suoran summan kanssa, missä nämä summattavat ovat $m_1, \ldots, m_t$ siten että $m_1 > 1$ ja $m_1 \mid m_2 \mid \ldots \mid m_t$.*

*Todistus.* Sivuutetaan. [4], Teoreema 2.1, s. 128. □

**Määritelmä 2.18.** Olkoon $G$ ryhmä ja $a$ jokin sen alkio. Olkoon ryhmällä $G$ lisäksi aliryhmä $H$. Tällöin joukko $aH = \{ah \mid h \in G\}$ on nimeltään aliryhmän $H$ *vasen sivuluokka* ja alkio $a$ tämän sivuluokan *edustaja*. Vasempien sivuluokkien joukkoa $\{aH \mid a \in G\}$ merkitään $G/H$ (Luonnollisesti $Ha = \{ha \mid h \in H\}$ on aliryhmän $H$ *oikea sivuluokka*.)

**Määritelmä 2.19.** Ryhmän $G$ aliryhmä $H$ on *normaali*, jos sen vasemmat ja oikeat sivuluokat ovat samat eli $gH = Hg$ kaikilla $g \in G$. Tällöin merkitään $H \trianglelefteq G$.

**Määritelmä 2.20.** Olkoon $G$ ei-triviaali-ryhmä. Ryhmää $G$ sanotaan *yksinkertaiseksi*, jos sen ainoat normaalit aliryhmät ovat triviaalit aliryhmät $\{e\}$ ja $G$.

**Lause 2.21.** *Olkoon $G$ ryhmä ja $H \leq G$. Aliryhmä $H$ on normaali, jos ja vain jos $ghg^{-1} \in H$ kaikilla $h \in H$ ja $g \in G$.*

*Todistus.* Olkoon $H$ normaali aliryhmä. Oletetaan, että $g \in G$ ja $h \in H$. Nyt $gh \in gH$, ja normaalin aliryhmän määritelmän nojalla $gH = Hg$, joten $gh \in Hg$. Siispä $gh = h'g$ jollakin $h' \in H$, mistä saadaan $ghg^{-1} = h' \in H$.

Oletetaan seuraavaksi, että $ghg^{-1} \in H$ kaikilla $h \in H$ ja $g \in G$. Olkoot $g \in G$ ja $h \in H$. Nyt $ghg^{-1} = h'$ jollakin $h' \in H$, joten $gh = h'g \in Hg$. Koska $h$ on mielivaltainen aliryhmän $H$ alkio, niin $gH \subset Hg$. Osoitetaan vielä, että pätee myös $Hg \subset gH$. Oletuksen nojalla $g^{-1}h(g^{-1})^{-1} = g^{-1}hg \in H$, joten $g^{-1}hg = h''$ jollakin $h'' \in H$. Kertomalla yhtälöä saadaan $hg = gh''$, josta seuraa, että $Hg \subset gH$. Näin on osoitettu, että $gH = Hg$, joten $H$ on normaali. □

**Lause 2.22.** *Ryhmähomomorfismin $f : G \to H$ ydin on lähtöjoukon $G$ normaali aliryhmä.*

*Todistus.* Olkoot $G$ ja $H$ ryhmiä ja $f : G \to H$ homomorfismi. Osoitetaan ensin, että ydin Ker$f$ on ryhmän $G$ aliryhmä. Käytetään todistuksessa lausetta 2.3. Määritelmän mukaan ydin on ryhmän $G$ osajoukko. Koska $f(e) = e$, niin neutraalialkio kuuluu ytimeen ja Ker$f$ on epätyhjä joukko. Olkoot $a, b \in$ Ker$f$, jolloin määritelmän mukaan $f(a) = f(b) = e$. Koska $f$ on ryhmähomomorfismi, niin $f(ab^{-1}) = f(a)f(b)^{-1} = ee^{-1} = e$ ja $ab^{-1} \in$ Ker$f$. Osoitetaan vielä, että tämä aliryhmä on normaali käyttämällä apuna edellä esitettyä lausetta 2.21. Olkoot $g \in G$ ja $h \in$ Ker$f$. Tällöin

$$\begin{aligned} f(ghg^{-1}) &= f(g)f(h)f(g^{-1}) = f(g)ef(g^{-1}) \\ &= f(g)f(g^{-1}) = f(gg^{-1}) \\ &= f(e) = e, \end{aligned}$$

joten $ghg^{-1} \in$ Ker$f$ ja ydin on normaali aliryhmä. □

**Lause 2.23.** *Olkoot $H$ ja $G$ ryhmän $G$ normaaleja aliryhmiä. Jos $HK = G$ ja $H \cap K = \{e\}$, niin $G \cong H \times K$.*

*Todistus.* Olkoon $G$ ryhmä ja $H \trianglelefteq G$ sekä $K \trianglelefteq G$. Osoitetaan ensin, että $hk = kh$ kaikilla $h \in H$ ja $k \in K$. Tämä on yhtäpitävää sen kanssa, että $hkh^{-1}k^{-1} = e$. Koska $K$ on ryhmän $G$ normaali aliryhmä niin lauseen 2.21 perusteella $hkh^{-1} \in K$, joten $(hkh^{-1})k^{-1} \in K$. Samalla tavalla $kh^{-1}k^{-1} \in H$ eli $h(kh^{-1}k^{-1}) \in H$. Kun nämä molemmat otetaan huomioon, niin $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ eli $hk = kh$.

Oletetaan, että $G = HK$ ja $H \cap K = \{e\}$. Tällöin jokaisella $g \in G$ on esitys $g = hk$, jossa $h \in H$ ja $k \in K$. Tämä esitys on yksikäsitteinen, sillä jos $g = hk = h'k'$, niin saadaan yhtäpitävästi $(h')^{-1}h = (k')^{-1}k$. Nyt alkio $(h')^{-1}h$ on ryhmässä $H$ ja $(k')^{-1}k$ ryhmässä $K$, joten ne molemmat ovat ryhmässä $H \cap K = \{e\}$, mistä seuraa, että $h = h'$ ja $k = k'$ eli esitys on yksikäsitteinen. Tällöin voidaan määritellä kuvaus $f : G \to H \times K$ kaavalla $f(hk) = (h, k)$. Näytetään, että tämä kuvaus on bijektio. Selvästikin $f$ on injektio, sillä

jos $f(hk) = (h,k) = (h',k') = f(h'k')$, niin $hk = h'k'$. Lisäksi kuvaus $f$ on surjektio, sillä jokaiselle maalijoukon mielivaltaiselle alkiolle $(h,k)$, löytyy alkio $g$ lähtöjoukosta $G$, kun valitaan $g = hk$. Osoitetaan vielä, että $f$ on homomorfismi. Koska ryhmien $H$ ja $K$ alkiot ovat keskenään vaihdannaisia, niin

$$f(hk \cdot h'k') = f(hh' \cdot kk') = (hh', kk') = (h,k) \cdot (h',k') = f(hk) \cdot f(h'k'),$$

joten kuvaus $f : G \to H$ on sekä bijektio että homomorfismi eli $G \cong H \times K$. □

**Lemma 2.24.** *Olkoon $H \leq G$ ja $a, b \in G$. Tällöin seuraavat ehdot pätevät:*

1. $a \in aH$
2. $aH = H \Leftrightarrow a \in H$
3. $aH = bH$ *tai* $aH \cap bH = \emptyset$
4. $aH = bH \Leftrightarrow a^{-1}b \in H$
5. $|aH| = |bH|$
6. $aH = Ha \Leftrightarrow H = a^{-1}Ha$
7. $aH \leq G \Leftrightarrow a \in H$.

*Todistus.* 1. $a = ae \in aH$, sillä $e \in H$.

2. Oletetaan ensin, että $aH = H$. Kohdan 1 perusteella $a \in aH$, joten $a \in H$. Oletetaan nyt, että $a \in H$. Selvästi $aH \subset H$, joten riittää osoittaa, että $H \subset aH$. Olkoon $h \in H$, jolloin $h = (aa^{-1})h = a(a^{-1}h) \in aH$, sillä $a^{-1}h \in H$.

3. Oletetaan, että $aH \cap bH \neq \emptyset$ ja osoitetaan, että tällöin pätee $aH = bH$. Olkoon $x \in aH \cap bH$. Siis on olemassa sellaiset $h_1, h_2 \in H$, joilla pätee $x = ah_1$ ja $x = bh_2$. Tällöin $ah_1 = bh_2$, josta saadaan $a = bh_2h_1^{-1}$. Kohdan 2 perusteella $aH = bh_2h_1^{-1}H = bH$, sillä $h_2h_1^{-1} \in H$.

4. Osoitetaan ensin $aH = bH \Leftrightarrow H = a^{-1}bH$. Oletetaan, että $aH = bH$. Koska $G$ on ryhmä ja $a \in G$, niin myös $a^{-1} \in G$. Kerrotaan yhtälön molemmat puolet vasemmalta alkiolla $a^{-1}$, jolloin saadaan $a^{-1}(aH) = a^{-1}(bH) \Rightarrow (a^{-1}a)H = (a^{-1}b)H \Rightarrow H = a^{-1}bH$ eli $aH = bH \Rightarrow H = a^{-1}bH$. Oletetaan seuraavaksi, että $H = a^{-1}bH$. Kerrotaan yhtälöä vasemmalta puolelta alkion $a^{-1}$ käänteisalkiolla. $H = a^{-1}bH \Rightarrow (a^{-1})^{-1}H = (a^{-1})^{-1}(a^{-1}bH) \Rightarrow aH = ((a^{-1})^{-1}a^{-1})bH \Rightarrow aH = bH$. Nyt on saatu osoitettua, että $aH = bH \Leftrightarrow H = a^{-1}bH$. Kohdan 2 perusteella puolestaan $H = a^{-1}bH \Leftrightarrow a^{-1}b \in H$, joten $aH = bH \Leftrightarrow a^{-1}b \in H$.

5. Osoittaakseen, että kaikki sivuluokat ovat yhtä mahtavia riittää osoittaa, että $|aH| = |H|$ kaikilla $a \in G$. Näytetään, että sivuluokan $H$ ja minkä tahansa muun sivuluokan välille voidaan määritellä bijektio. Olkoon $aH$ jokin aliryhmän $H$ sivuluokista. Määritellään kuvaus $f : H \to aH$ siten että $f(x) = ax$ kaikilla $x \in H$. Osoitetaan, että näin määritelty kuvaus todella on bijektio. Tämä voidaan tehdä helposti etsimällä kuvaukselle $f$ käänteiskuvaus. Olkoon $g : aH \to H$, $g(x) = a^{-1}x$ kaikilla $x \in aH$. Selvästikin $a^{-1}x \in H$, sillä $x$ on muotoa $ah$, missä $h \in H$ ja $a \in G$, jolloin $a^{-1}x = a^{-1}ah = eh = h \in H$. Nyt $f(g(x)) = f(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = x$ ja $g(f(x)) = g(ax) = a^{-1}(ax) = (a^{-1}a)x = x$. Siis $g$ on kuvauksen $f$ käänteiskuvaus ja $f$ on bijektio.

6. Oletetaan aluksi, että $aH = Ha$. Kerrotaan yhtälön molemmat puolet alkion $a$ käänteisalkiolla ja saadaan $a^{-1}aH = a^{-1}Ha$, mistä seuraa, että $H = a^{-1}Ha$. Oletetaan nyt, että $H = a^{-1}Ha$ ja kerrotaan vasemmalta puolelta alkiolla $a$. Näin saadaan $aH = a(a^{-1}Ha) = (aa^{-1})Ha = Ha$. Nyt on saatu osoitettua, että $aH = Ha \Leftrightarrow H = a^{-1}Ha$.

7. Jos $aH \leq G$, niin tiedetään, että $e \in aH$. Tällöin $aH \cap eH \neq \emptyset$, joten kohdan 3 perusteella $aH = eH = H$. Nyt voidaan käyttää kohtaa 2 ja saadaan $a \in H$. Oletetaan seuraavaksi, että $a \in H$. Tällöin kohdan 2 perusteella $aH = H \leq G$, joten $aH \leq G \Leftrightarrow a \in H$.

□

**Määritelmä 2.25.** Olkoon $G$ ryhmä ja $H$ sen aliryhmä. Tällöin aliryhmän $H$ *indeksiksi* kutsutaan sen vasempien sivuluokkien lukumäärää ja merkitään $[G : H]$.

**Lause 2.26.** *Olkoon $G$ ryhmä ja $H$ sen aliryhmä. Jos aliryhmän $H$ indeksi on kaksi, niin $H$ on ryhmän $G$ normaali aliryhmä.*

*Todistus.* Olkoon $G$ ryhmä, $H$ sen aliryhmä ja $[G : H] = 2$. Olkoon $h \in H$ ja $a, g \in G$ siten että $a \notin H$. Tällöin $aH$ on eri sivuluokka kuin $H$. Koska sivuluokkia on vain kaksi, niin $G = H \cup aH$. Jos $g \in H$, niin selvästi $ghg^{-1} \in H$ ja lauseen 2.21 perusteella $H$ on normaali aliryhmä. Oletetaan nyt, että $g \neq H$. Tällöin $g \in aH$ eli on olemassa $k \in H$, siten että $g = ak$. Nyt halutaan osoittaa, että $ghg^{-1} \in H$, joten tehdään vastaoletus, että $ghg^{-1} \notin H$. Tällöin $ghg^{-1} = akh(ak)^{-1} \in aH$ ja siis $akhk^{-1}a^{-1} = ah'$ jollakin $h' \in H$. Tästä seuraa

$$\begin{aligned} & khk^{-1}a^{-1} = h' \text{ jollakin } h' \in H \\ \Rightarrow\ & khk^{-1} = h'a \text{ jollakin } h' \in H \\ \Rightarrow\ & (h')^{-1}khk^{-1} = a \text{ jollakin } h' \in H. \end{aligned}$$

Koska $(h')^{-1}khk^{-1} \in H$, niin $a \in H$, mikä on ristiriidassa oletuksen kanssa. Täytyy siis päteä, että $ghg^{-1} \in H$ ja $H$ on normaali aliryhmä. □

**Määritelmä 2.27.** Olkoon $G$ ryhmä. Tällöin sanotaan, että $G$ *toimii joukossa* $S$, jos on olemassa funktio $\Phi : G \times S \to S,\ \Phi(g, x) = gx$, jolle pätee kaikilla $x \in S$ ja $g_1, g_2 \in G$ seuraavat ehdot:

**(T1)** $ex = x$

**(T2)** $(g_1 g_2)x = g_1(g_2 x)$.

Tällä tavoin määriteltyä toimintaa kutsutaan *vasemmanpuoleiseksi toiminnaksi.*

**Esimerkki 2.28.** Olkoon $G$ ryhmä ja $H$ sen aliryhmä. Tällöin kuvaus

$$\Phi : G \times G/H \to G/H,\ (g', gH) \mapsto (g'g)H$$

määrittelee ryhmän $G$ toiminnan aliryhmän $H$ sivuluokkien joukossa.

**Esimerkki 2.29.** Ryhmässä $G$ voidaan määritellä toiminta

$$f_g : h \mapsto ghg^{-1},$$

jota kutsutaan ryhmän $G$ *konjugointitoiminnaksi* ja alkion kuvia tässä toiminnassa vastaavasti *konjugaateiksi.*

**Lause 2.30.** *Olkoon $G$ äärellinen ryhmä, $a$ jokin sen alkio ja $n \in \mathbb{Z}$. Tällöin*

$$a^n = e \Leftrightarrow (bab^{-1})^n = e \ \ \forall\ b \in G.$$

*Toisin sanoen alkion $a$ kertaluku on sama kuin sen konjugaatin kertaluku.*

*Todistus.* Olkoon $G$ ryhmä ja $a \in G$. Oletetaan ensin, että $a^n = e$ jollakin $n \in \mathbb{Z}$. Tällöin

$$(bab^{-1})^n = b^n a^n b^{-n} = b^n e b^{-n} = b^n b^{-n} = e.$$

Jos puolestaan $(bab^{-1})^n = e$, niin

$$\begin{aligned} & b^n a^n b^{-n} = e \\ \Leftrightarrow\ & a^n b^{-n} = b^{-n} \\ \Leftrightarrow\ & a^n = b^{-n}(b^{-n})^{-1} \\ \Leftrightarrow\ & a^n = e. \end{aligned}$$

Näin on osoitettu, että $a^n = e \Leftrightarrow (bab^{-1})^n = e$. □

**Lause 2.31.** *Jos ryhmä $G$ toimii joukossa $S$, niin tämä toiminta indusoi homomorfismin $G \to A(S)$, jossa $A(S)$ on ryhmä, joka koostuu joukon $S$ kaikista permutaatioista ja jonka laskutoimituksena on kuvausten yhdistäminen.*

*Todistus.* Olkoon $g \in G$. Määritellään kuvaus $\tau_g : S \to S$, niin että $x \mapsto gx$. Kuvaus $\tau_g$ on surjektio, sillä jos $x \in S$, niin myös $g^{-1}x \in S$ ja $g^{-1}x \mapsto g(g^{-1}x) = (gg^{-1})x = x$. Lisäksi $\tau_g$ on injektio, sillä jos $gx = gy$ $(x, y \in S)$, niin $x = g^{-1}(gx) = g^{-1}(gy) = y$. Näin ollen kuvaus $\tau_g$ on bijektio. Koska $\tau_{gg'}(x) = (gg')x = g(g'x) = \tau_g\tau_{g'}(x)$, kun $g, g' \in G$, niin kuvaus $G \to A(S)$, joka kuvaa alkion $g$ alkioksi $\tau_g$, on homomorfismi. □

**Lause 2.32.** *Olkoon $H$ ryhmän $G$ aliryhmä ja joukko $S$ aliryhmän $H$ kaikkien vasempien sivuluokkien joukko. Olkoon lisäksi joukossa $S$ määritelty ryhmän $G$ toiminta vasemmalta puolelta kuten esimerkissä 2.28. Tällöin homomorfismin $G \to A(S)$ ydin sisältyy aliryhmään $H$.*

*Todistus.* Indusoitu homomorfismi $G \to A(S)$ kuvaa alkion $g$ alkiolle $\tau_g$, kun $\tau_g : S \to S$ ja $\tau_g(xH) = gxH$. Jos $g$ kuuluu yllä määritellyn homomorfismin ytimeen, niin $\tau_g = id$ eli $g \mapsto id$, jolloin $gxH = xH$ kaikilla $x \in G$. Valitaan $x = e \in G$. Nyt yhtälö saa muodon $geH = eH$, joten $gH = H$ ja lemman 2.24 perusteella $g \in H$ eli homomorfismin ydin sisältyy aliryhmään $H$. □

**Määritelmä 2.33.** Olkoon $G$ ryhmä ja oletetaan, että ryhmän $G$ toiminta on määritelty joukossa $S$. Tällöin alkion $x \in S$ *rata* on joukko

$$Gx = \{gx \mid g \in G\}.$$

**Määritelmä 2.34.** Olkoon $G$ ryhmä ja $x \in G$. Alkion $x$ *keskittäjä* ryhmässä $G$ koostuu niistä alkioista, jotka kommutoivat alkion $x$ kanssa ja sitä merkitään

$$\begin{aligned} C_G(x) &= \{g \in G \mid gxg^{-1} = x\} \\ &= \{g \in G \mid gx = xg\}. \end{aligned}$$

**Määritelmä 2.35.** Keskittäjien leikkaus on nimeltään *keskus* ja merkitään

$$\begin{aligned} Z(G) = \bigcap_{x \in G} C_G(x) &= \{g \in G \mid gxg^{-1} = x \text{ kaikilla } x \in G\} \\ &= \{g \in G \mid gx = xg \text{ kaikilla } x \in G\}. \end{aligned}$$

Keskuksen alkiot kommutoivat ryhmän $G$ kaikkien alkioiden kanssa.

**Lause 2.36.** *Olkoon $G$ ryhmä ja olkoon $C$ jokin tämän ryhmän konjugaattiluokkien edustajisto eli joukkoon $C$ on valittu täsmälleen yksi edustaja jokaisesta konjugaattiluokasta. Tällöin pätee*

$$|G| = |Z(G)| + \sum_{\substack{x \in C \\ x \notin Z(G)}} [G : C_{G(x)}].$$

*Todistus.* Sivuutetaan. [6], lause 2.12, s. 25. □

# Luku 3

# Lagrangen lause

Tässä luvussa esittelen ryhmäteorian kannalta erittäin tärkeän lauseen, jonka Joseph Louis Lagrange esitti ensimmäisen kerran jo 1770-luvulla, vaikka ryhmäteorian käsitettä ei tuolloin vielä edes tunnettu. Lauseen täydellisen todistuksen onnistui tosin esittämään vasta 30 vuotta myöhemmin Pietro Abbati. ([3], s. 128.) Lisäksi todistan Lagrangen lauseeseen läheisesti liittyvät korollaarit.

**Lause 3.1.** *Jos $G$ on äärellinen ryhmä ja $H$ sen aliryhmä, niin aliryhmän $H$ kertaluku $|H|$ jakaa ryhmän $G$ kertaluvun $|G|$.*

*Todistus.* Olkoon $G$ ryhmä ja $H$ sen aliryhmä. Olkoot lisäksi $a_1H, a_2H, \ldots, a_rH$ aliryhmän vasemmat sivuluokat. Tällöin kaikille $a \in G$ on olemassa indeksi $i$ siten että $aH = a_iH$ jollakin $i \in \{1, \ldots, r\}$. Lemman 2.24 ensimmäisen kohdan perusteella $a \in aH$. Jokainen ryhmän $G$ alkio kuuluu johonkin aliryhmän $H$ sivuluokkaan $a_iH$ ja $G$ on näiden sivuluokkien yhdiste eli $G = a_1H \cup a_2H \cup \ldots \cup a_rH$. Lemman 2.24 kolmannen kohdan perusteella sivuluokat ovat erillisiä, joten ryhmän $G$ kertaluku on näiden sivuluokkien kertalukujen summa eli $|G| = |a_1H| + |a_2H| + \ldots + |a_rH|$. Käytetään lemman 2.24 viidettä kohtaa, jonka mukaan kaikkien sivuluokkien kertaluku on sama. Saadaan, että $|a_iH| = |H|$ kaikilla $i \in \{1, \ldots, r\}$, joten $|G| = r|H|$ ja aliryhmän $H$ kertaluku jakaa ryhmän $G$ kertaluvun. □

**Korollaari 3.2.** *Olkoon $G$ äärellinen ryhmä ja $H$ sen aliryhmä. Tällöin aliryhmän $H$ indeksi eli vasempien sivuluokkien määrä on ryhmän $G$ ja sen aliryhmän $H$ kertalukujen osamäärä. Toisin sanoen*

$$[G : H] = \frac{|G|}{|H|}.$$

*Todistus.* Korollaari seuraa suoraan Lagrangen lauseen todistuksesta, sillä havaitaan, että aliryhmän $H$ vasempien sivuluokkien määrä on todistuksen tapauksessa $r$ ja

$$r = \frac{|G|}{|H|}.$$

□

**Korollaari 3.3.** *Äärellisessä ryhmässä jokaisen alkion kertaluku jakaa ryhmän kertaluvun.*

*Todistus.* Olkoon $G$ äärellinen ryhmä ja $a$ jokin sen alkio. Selvästikin alkion kertaluku on sama kuin sen virittämän ryhmän alkioiden lukumäärä eli $|a| = |\langle a \rangle|$ ja lisäksi $\langle a \rangle \leq G$. Tällöin Lagrangen lauseen mukaan alkion $a$ virittämän ryhmän kertaluku (joka on sama kuin alkion $a$ kertaluku) jakaa ryhmän $G$ kertaluvun. □

**Korollaari 3.4.** *Ryhmä, jonka kertaluku on jaoton, on syklinen.*

*Todistus.* Olkoon $G$ ryhmä siten että $|G|$ on jaoton. Olkoon $a$ jokin ryhmän $G$ alkioista ja $a \neq e$.(Jos ryhmässä $G$ on ainoastaan neutraalialkio, niin todistus on selvä, sillä tällöin $G = \langle e \rangle$.) Alkion $a$ virittämän aliryhmän kertaluku $|\langle a \rangle|$ jakaa ryhmän $G$ kertaluvun $|G|$ ja $|\langle a \rangle| \neq 1$. Koska $|G|$ on jaoton, niin täytyy päteä, että $|\langle a \rangle| = |G|$. Alkio $a$ virittää siis koko ryhmän $G$ ja $G$ on syklinen. □

**Korollaari 3.5.** *Olkoon $G$ äärellinen ryhmä ja $a$ jokin sen alkio. Tällöin $a^{|G|} = e$.*

*Todistus.* Olkoon $G$ äärellinen ryhmä ja $a \in G$. Nyt korollaarin 3.3 perusteella $|G| = |a|k$ jollakin $k \in \mathbb{N}$. Siis $a^{|G|} = a^{|a|k} = (a^{|a|})^k = e^k = e$. □

# Luku 4

# Sylowin lauseet

Lagrangen lauseen mukaan äärellisen ryhmän jokaisen aliryhmän kertaluku jakaa aina ryhmän kertaluvun. Entä päteekö tämä toiseen suuntaan? Onko mahdollista löytää jokaista ryhmän kertaluvun tekijää kohti aliryhmä, jonka kertaluku olisi tämä tekijä? Yleisessä tapauksessa näin ei päde. Augustin Louis Cauchy todisti vuonna 1845, että tälläinen aliryhmä löytyy aina jokaista alkulukua olevaa tekijää kohti. Vuonna 1872 Peter Sylow osoitti, että itse asiassa jokaista ryhmän kertaluvun tekijää kohti, joka on jokin alkuluvun potenssi, löytyy aliryhmä, jonka kertaluku on tämä alkuluvun potenssi. ([6], s. 37.) Tässä luvussa esittelen tarkemmin nämä Sylowin lauseina tunnetut tulokset.

**Lause 4.1.** *Olkoon $G$ äärellinen ryhmä, jonka kertaluku on jaollinen alkuluvulla $p$. Tällöin ryhmä $G$ sisältää alkion, jonka kertaluku on $p$.*

*Todistus.* Sivuutetaan. [4], Teoreema 5.2. s. 93. □

**Määritelmä 4.2.** Oletetaan, että ryhmän kertaluku on $p^k m$, missä $p$ on alkuluku, $k \geq 1$ ja $m$ ei ole jaollinen luvulla $p$. Sellaista aliryhmää, jonka kertaluku on $p^k$, kutsutaan *Sylowin $p$-aliryhmäksi.*

**Lause 4.3.** *Oletetaan, että $|G| = p^k m$, missä $k \geq 1$ ja $p$ on alkuluku, joka ei jaa lukua $m$. Tällöin*

**(i)** *Ryhmällä $G$ on Sylowin $p$-aliryhmä.*

**(ii)** *Ryhmän $G$ Sylowin $p$-aliryhmät ovat keskenään konjugaatteja.*

**(iii)** *Jos $s_p$ on Sylowin $p$-aliryhmien lukumäärä, niin $s_p \equiv 1 \pmod{p}$ ja $s_p$ jakaa luvun $m$.*

*Todistus.* Sylowin lauseille voi löytää useampia erilaisia todistuksia kirjallisuudesta. Sylow itse käytti todistuksessaan Cauchyn löytämiä tuloksia. Jokke Häsän luentomateriaalista Algebra II (Matematiikan ja tilastotieteen laitos, kevät 2010, Helsingin yliopisto) voi puolestaan löytää Helmut Wielandtin kombinatoriseen havaintoon perustuvan esityksen todistuksesta (s. 38). Tässä Pro Gradu -tutkielmassa todistus sivuutetaan. [6] □

# Luku 5

# Diedriryhmät

Tässä luvussa esittelen symmetrisen ryhmän käsitteen ja sen myötä diedriryhmän $D_n$, kun $n \geq 3$. Näihin ryhmiin tulen palaamaan seuraavissa luvuissa.

Merkitään $n$ ensimmäisen positiivisen kokonaisluvun joukkoa $N_n = \{1, 2, \ldots, n\}$. Tämän joukon kaikkien permutaatioiden muodostamaa ryhmää kutsutaan *symmetriseksi ryhmäksi* $S_n$ ja laskutoimituksena toimii permutaatioiden tulo. Esimerkkinä tästä lukujen 1,2 ja 3 permutaatioista koostuva ryhmä $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Tarkastellaan symmetrisen ryhmän $S_n (n \geq 3)$ aliryhmää $D_n$, jonka virittävät alkiot $a = (123 \cdots n)$ ja

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Tätä aliryhmää $D_n$ kutsutaan *diedriryhmäksi*. Diedriryhmä $D_n$ voidaan ajatella myös säännöllisen $n$-kulmion symmetriaryhmänä, jolloin virittäjäalkio $a$ vastaa monikulmion kiertoa kulman $2\pi/n$ verran ja alkio $b$ peilausta jonkin symmetria-akselin suhteen.

Olkoon $n \geq 3$. Näytetään, että tällöin diedriryhmä $D_n$ on ryhmä, jonka kertaluku on $2n$ ja jonka virittävät alkiot $a$ ja $b$, joille pätee

1. $a^n = (1); b^2 = (1); a^k \neq (1)$ jos $0 < k < n$;
2. $ba = a^{-1}b$.

Lisäksi osoitetaan, että jokainen ryhmä $G$, jonka virittäjäalkiot toteuttavat ehdot 1. ja 2. jollakin $n \geq 3$, on isomorfinen ryhmän $D_n$ kanssa. Alkio (1) luonnollisesti korvataan ryhmän $G$ neutraalialkiolla $e$. Huomataan ensiksi, että

$$(123 \cdots n)^n = \underbrace{(123 \cdots n)(123 \cdots n) \ldots (123 \cdots n)}_{n \text{ kpl}} = (1)(2) \ldots (n) = (1)$$

ja toisaalta $(123\cdots n)^k \neq (1)$ jos $0 < k < n$. Lisäksi pätee

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}^2 = (1)(2)\ldots(n) = (1).$$

Yllä esitellyt alkiot $a = (123\cdots n)$ ja

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}$$

siis toteuttavat ehdon 1. Tarkistetaan vielä 2. ehto:

$$\begin{aligned} ba &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} (123\cdots n) \\ &= (1\ n)(2\ (n-1))(3\ (n-2))\ldots((n-2)\ 3)((n-1)\ 2) \end{aligned}$$

$$\begin{aligned} a^{-1}b &= (n\ n-1\ldots 3\ 2\ 1) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} \\ &= (1\ n)(2\ (n-1))(3\ (n-2))\ldots((n-2)\ 3)((n-1)\ 2), \end{aligned}$$

jolloin huomataan, että $ba = a^{-1}b$ ja jälkimmäinen ehdoista pätee myös. Koska alkiot $a$ ja $b$ virittävät ryhmän $D_n$, niin kaikki tämän ryhmän alkiot voidaan kirjoittaa muodossa $a^{m_1}b^{m_2}a^{m_3}b^{m_4}\ldots a^{m_{k-1}}b^{m_k}$ ($m_i \in \mathbb{Z}$). Lisäksi todettiin, että $ba = a^{-1}b = a^{n-1}b$, jolloin kaikki alkiot voidaan järjestää muotoon $a^ib^j$, missä $i \in \{0, 1, \ldots, n-1\}$ ja $j \in \{0, 1\}$, sillä $a^n = e$ ja $b^2 = e$. Erilaisia kombinaatioita on $2n$ kappaletta. Osoitetaan, että nämä kaikki $2n$ alkiota ovat erillisiä. Ensinnäkin huomataan, että $a^i(1) = (123\cdots n)^i(1) = i+1$. Tällöin

$$a^j(1) = (123\cdots n)^j(1) = j + 1 \neq i + 1 = a^i(1),$$

jos $i, j \in \{0, 1, \ldots n-1\}$ ja $i \neq j$. Alkiot $a^i$ ja $a^j$ ovat siis eri alkiot, jos $i \neq j$. Toisaalta

$$b(1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} (1) = 1,$$

jolloin $a^jb(1) = a^j(1) = j + 1$ ja $a^i(1) \neq a^jb(1)$, kun $i, j \in \{0, 1, \ldots n-1\}$ ja $i \neq j$ eli tällöin $a^i \neq a^jb$. Tutkitaan vielä tapaus $i = j$. Huomataan, että $b(2) = n$, joten $a^ib(2) = a^i(n) = i + n$ ja lisäksi $a^i(2) = i + 2$ eli $a^ib \neq a^i$, kun $i \in \{0, 1, \ldots n-1\}$ ja $n \geq 3$. Viimeiseksi tulee osoittaa, että $a^ib \neq a^jb$. Tehdään vastaoletus, että $a^ib = a^jb$, kun $i, j \in \{0, 1, \ldots n-1\}$ ja $i \neq j$. Tällöin $a^i = a^j$, mikä on ristiriita, sillä ylempänä osoitimme, että $a^i \neq a^j$, joten $a^ib \neq a^jb$. Kaikki $2n$ alkiota ovat siis erillisiä.

Olkoon nyt $G$ ryhmä, jonka virittävät alkiot $a$ ja $b$, jotka toteuttavat ehdot 1. ja 2. jollakin $n \geq 3$. Tällöin ryhmän $G$ alkiot voidaan kirjoittaa muodossa $a^{m_1}b^{m_2}a^{m_3}b^{m_4}\dots a^{m_{k-1}}b^{m_k}$ ($m_i \in \mathbb{Z}$). Tiedetään, että $a^{-1}b = ba$ sekä $a^n = e$ ja $b^2 = e$, jolloin kaikki ryhmän $G$ alkiot voidaan esittää muodossa $a^ib^j$, missä $i \in \{0, 1, \dots, n-1\}$ ja $j \in \{0, 1\}$.

Käytetään ryhmän $D_n$ virittäjille merkintää $a_i, b_j$, jotta vältytään sekaannuksilta. Osoitetaan, että ryhmät $G$ ja $D_n$ ovat isomorfiset. Tämän osoittamiseksi näytetään, että kuvaus $f : D_n \to G, a_1^ib_1^j \mapsto a^ib^j$ on bijektio. Selvästikin $f$ on surjektio, sillä kaikille $a^ib^j \in G$ löytyy $a_1^ib_1^j \in D_n$ siten että $f(a_1^ib_1^j) = a^ib^j$. Injektiivisyyden osoittamiseksi riittää lauseen 2.14 perusteella osoittaa, että $\ker f = \{e\}$. Oletetaan, että $f(a_1^ib_1^j) = a^ib^j = e$, jollakin $i \in \{0, 1, \dots n-1\}$ ja $j \in \{0, 1\}$. Jos $j = 1$, niin

$$a^ib = e \Leftrightarrow a^ib^2 = eb \Leftrightarrow a^i = b.$$

Käytetään hyväksi tätä tietoa sekä ehtoa 2., jolloin saadaan

$$a^{i+1} = a^ia = ba = a^{-1}b = a^{-1}a^i = a^{i-1}.$$

Toisin sanoen

$$a^{i+1} = a^{i-1} \Leftrightarrow a^ia = a^ia^{-1} \Leftrightarrow a = a^{-1} \Leftrightarrow a^2 = e.$$

Tämä on ristiriita, sillä oletimme, että $n \geq 3$, joten $j = 0$ ja $e = a^ib^0 = a^i$ jollakin $i \in \{0, 1, \dots n-1\}$. Ehdosta 1. seuraa, että $i = 0$, joten $f(a_1^ib_1^j) = e$ implikoi $a_1^ib_1^j = a_1^0b_1^0 = (1)$. Tällöin $\ker f = \{e\}$ ja kuvaus $f$ on injektio eli myös bijektio ja $G \cong D_n$.

# Luku 6

# Kertaluvut 1, 2, 3, 5, 7, 11 ja 13

Yksinkertaisin algebrallinen ryhmä on luonnollisesti triviaali ryhmä, joka sisältää vain neutraalialkion $e$. Tällainen ryhmä on esimerkiksi syklinen ryhmä $Z_1 = [0]_1$. Koska ryhmän täytyy sisältää ainakin neutraalialkio, niin kaikki muut yhden alkion ryhmät ovat isomorfisia tämän ryhmän kanssa.

Korollaarin 3.4 mukaan jokainen ryhmä, jonka kertaluku on alkuluku, on syklinen. Toisaalta lauseen 2.15 todistuksessa osoitettiin, että jokainen syklinen ryhmä, jonka kertaluku on $n$, on isomorfinen ryhmän $Z_n$ kanssa. Näin ollen kertalukuja 2,3,5,7,11 ja 13 olevia ryhmiä on kaikkia täsmälleen yksi ja nämä ryhmät ovat $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}$ ja $\mathbb{Z}_{13}$.

# Luku 7

# Kertaluvut 4 ja 9

Lauseen 2.17 avulla saadaan mahdolliset kertalukua 4 olevat Abelin ryhmät, jotka ovat $\mathbb{Z}_4$ ja $\mathbb{Z}_2 \times \mathbb{Z}_2$. Nämä ryhmät eivät ole keskenään isomorfisia, sillä ryhmä $\mathbb{Z}_4$ on selvästi syklinen, kun taas ryhmässä $\mathbb{Z}_2 \times \mathbb{Z}_2$ neutraalialkiota lukuun ottamatta kaikki alkiot ovat kertalukua kaksi. Tämä voidaan osoittaa seuraavasti: Olkoon $a, b \in \mathbb{N}$. Tällöin $2([a]_2, [b]_2) = ([2a]_2, [2b]_2) = ([0]_2, [0]_2) = e$, sillä luvut $2a$ ja $2b$ ovat jaollisia kahdella. Näin ollen $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Samalla tavalla voidaan löytää kertalukua 9 olevat Abelin ryhmät. Jälleen vaihtoehtoja on kaksi: ryhmät $\mathbb{Z}_9$ ja $\mathbb{Z}_3 \times \mathbb{Z}_3$. Yllä esitetyllä tavalla voidaan osoittaa, että nämä ryhmät eivät ole isomorfisia, sillä $\mathbb{Z}_9$ on syklinen ja ryhmän $\mathbb{Z}_3$ kaikkien alkioiden kertaluku on 3 neutraalialkiota lukuunottamatta.

Osoitetaan yleisesti, että jos $p$ on alkuluku, niin jokainen ryhmä, jonka kertaluku on $p^2$ on vaihdannainen. Tällöin ainoat kertalukua 4 olevat ryhmät olisivat $\mathbb{Z}_4$ ja $Z_2 \times Z_2$ ja kertalukua 9 olevat ryhmät puolestaan $Z_9$ ja $Z_3 \times Z_3$. Todistuksen helpottamiseksi näytetään ensin, että jos $p$ on alkuluku, niin jokaisen $p$-ryhmän $G$ keskus $Z(G)$ on epätriviaali.

Olkoon $p$ alkuluku. Olkoon $G$ jokin $p$-ryhmä ja $x$ sen alkio. Jos $x \in Z(G)$, niin $x$ kommutoi ryhmän $G$ kaikkien alkioiden kanssa eli $xg = gx$ kaikilla $g \in G$. Tällöin siis keskittäjä $C_G(x)$ on koko ryhmä $G$. Toisaalta jos $C_G(x) = G$, niin alkion $x$ kanssa kommutoivat kaikki alkiot $g \in G$ eli $x \in Z(G)$. Nyt pätee

$$x \in Z(G) \Leftrightarrow C_G(x) = G.$$

Jos $C_G(x) = G$, niin keskittäjällä $C_G(x)$ on vain yksi sivuluokka ryhmässä $G$. Implikaatio pätee myös toiseen suuntaan, sillä jos $[G : C_G(x)] = 1$, niin kaikki ryhmän $G$ alkiot kuuluvat myös keskittäjään $C_G(x)$. Kaiken kaikkiaan nyt on osoitettu seuraavat ekvivalenssit:

$$x \in Z(G) \Leftrightarrow C_G(x) = G \Leftrightarrow [G : C_G(x)] = 1.$$

Oletimme, että $G$ on $p$-ryhmä, jolloin sen kertaluku on $p^m$ jollakin $m \in \mathbb{N}$. Korollaarista 3.2 seuraa tällöin, että

$$[G : C_G(x)] = \frac{|G|}{|C_G(x)|} = \frac{p^m}{|C_G(x)|} \text{ jollakin } m \in \mathbb{N},$$

jolloin $[G : C_G(x)] \mid p^m$. Koska $p$ on alkuluku, niin $[G : C_G(x)] \in \{1, p, \ldots, p^m\}$. Jos $Z(G)$ olisi triviaali eli $Z(G) = \{e\}$, niin löytyisi täsmälleen yksi alkio $x \in G$, jolle pätisi $[G : C_G(x)] = 1$. Tämä alkio olisi luonnollisesti ryhmän $G$ neutraalialkio $e$. Tällöin lauseessa 2.36 esitelty luokkayhtälö

$$|G| = |Z(G)| + \sum_{\substack{x \in C \\ x \notin Z(G)}} [G : C_{G(x)}]$$

saisi muodon

$$p^m = 1 + p^{k_1} + p^{k_2} + \ldots + p^{k_r},$$

missä $k_1, \ldots, k_r \geq 1$. Tämä on kuitenkin ristiriita, joten keskus $Z_G(x)$ ei ole triviaali.

Osoitetaan vielä pieni aputulos ennen varsinaisen väitteen todistamista. Olkoon $G$ ryhmä ja $Z(G)$ sen keskus. Osoitetaan, että jos $G/Z(G)$ on syklinen niin ryhmä $G$ on vaihdannainen. Oletetaan, että $G/Z(G)$ on syklinen ja sen virittää alkio $gZ(G)$. Olkoot $x, y \in G$. Tällöin väite kuuluu $xy = yx$. Nyt $x \in xZ(G)$ ja $y \in yZ(G)$. Koska ryhmä $G/Z(G)$ on syklinen, niin $xZ(G) = g^m Z(G)$ ja $yZ(G) = g^n Z(G)$ joillakin $m, n \in \mathbb{N}$. Siispä $x = g^m z_1$ ja $y = g^n z_2$ joillakin $z_1, z_2 \in Z(G)$. Alkiot $z_1$ ja $z_2$ kommutoivat siis keskuksen määritelmän mukaan ryhmän $G$ kaikkien alkioiden kanssa, jolloin

$$xy = g^m z_1 g^n z_2 = g^m g^n z_1 z_2 = g^n g^m z_2 z_1 = g^n z_2 g^m z_1 = yx$$

ja ryhmä $G$ on vaihdannainen.

Nyt voidaan vihdoin osoittaa, että jos $p$ on alkuluku ja $G$ on ryhmä, jonka kertaluku on $p^2$, niin $G$ on Abelin ryhmä. Olkoon $|G| = p^2$. Edellä osoitettiin, että tällöin ryhmän $G$ keskus ei ole triviaali eli $Z(G) \neq \{e\}$. Lauseesta 3 seuraa, että $|Z(G)| = p$ tai $|Z(G)| = p^2$. Jos $|Z(G)| = p^2$, niin $Z(G) = G$ eli ryhmä $G$ on vaihdannainen. Jos puolestaan $|Z(G)| = p$, niin korollaarista 3.2 saadaan

$$|G/Z(G)| = [G : Z(G)] = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p.$$

Koska $p$ on alkuluku, niin korollaarin 3.4 perusteella tekijäryhmä $G/Z(G)$ on syklinen. Edellä osoitettiin, että tällöin ryhmä $G$ on vaihdannainen. Erityisesti siis kertalukua 4 ja 9 olevat ryhmät ovat Abelin ryhmiä ja nämä ryhmät esiteltiin tämän luvun alussa.

# Luku 8

# Kertaluvut 6, 10 ja 14

Tässä luvussa osoitan, että kertalukua 6, 10 ja 14 olevia ryhmiä on kaikkia täsmälleen kaksi. Huomataan, että $6 = 2 \cdot 3, 10 = 2 \cdot 5$ ja $14 = 2 \cdot 7$, joten näiden ryhmien kertaluvut ovat muotoa $2p$ jollakin alkuluvulla $p$. Olkoon $G$ ryhmä siten että $|G| = 2p$ ja $p$ on alkuluku. Voidaan myös olettaa, että $p \neq 2$. Tällöin lauseen 4.3 mukaan ryhmällä $G$ on Sylowin $p$-aliryhmä ja niiden lukumäärälle $s_p$ pätee $s_p \equiv 1 \pmod{p}$ ja $s_p$ jakaa luvun 2. Ainoa vaihtoehto on siis, että näitä Sylowin $p$-aliryhmiä on vain yksi kappale. Olkoon tämä kertalukua $p$ oleva aliryhmä $K$.

Tutkitaan nyt Sylowin 2-aliryhmiä. Koska näiden aliryhmien lukumäärälle $s_2$ pätee $s_2 \equiv 1 \pmod{2}$ ja $s_2 \mid p$, niin $s_2 = 1$ tai $s_2 = p$. Oletetaan ensin, että näitä aliryhmiä on vain yksi ja merkitään sitä $H$. Koska Sylowin 2-aliryhmät ovat keskenään konjugaatteja ja oletettiin, että niitä on vain yksi kappale, aliryhmän $H$ täytyy olla normaali. Sama pätee myös Sylowin $p$-aliryhmälle $K$. Lauseen 3.3 perusteella ryhmän alkion kertaluvun tulee jakaa koko ryhmän kertaluku, joten ryhmässä $K$ kaikkien alkioiden kertaluku on $p$ neutraalialkiota lukuunottamatta. Tästä seuraa, että $H \cap K = \{e\}$. Lisäksi $p$ ja 2 ovat alkulukuja ja niiden pienin yhteinen monikerta on $2p$, joten $|H||K| = 2p = |G|$. Lauseen 2.23 perusteella $G \cong H \times K$. Koska aliryhmien $H$ ja $K$ kertaluvut ovat alkulukuja, niin korollaarin 3.4 mukaan ne ovat syklisiä. Lisäksi lauseen 2.16 perusteella tiedetään, että ryhmä $H \times K$ on tällöin myös syklinen ja isomorfinen ryhmän $\mathbb{Z}_{2p}$ kanssa.

Oletetaan seuraavaksi, että Sylowin 2-aliryhmiä on $p$ kappaletta. Olkoon $K = \langle a \rangle$, missä $a^p = e$. Aliryhmä $K$ on ainoa kertalukua $p$ oleva aliryhmä, jolloin jos $b \notin K$, niin $b^2 = e$. Sivuluokat $K$ ja $bK$ ovat erillisiä ja sisältävät $p$ alkiota, joten $G = K \cup bK$. Ryhmä $G$ koostuu siis seuraavista erillisistä alkioista:

$$1, a, a^2, \ldots, a^{p-1}, b, ba, ba^2, \ldots, ba^{p-1}.$$

Jos $i \in \{0, 1, \ldots, p-1\}$, niin $(ba^i)^2 = e$, sillä $ba^{-1} \notin K$ ja kaikki ryhmän $G$ alkiot, jotka

eivät ole aliryhmässä $K$ ovat kertalukua 2. Lisäksi yhtälöstä $(ba^i)^2 = (ba^i)(ba^i) = e$ seuraa

$$ba^i = (ba^i)^{-1} = (a^i)^{-1}b^{-1} = a^{p-1}b.$$

Tutkitaan seuraavaksi ryhmää $G'$, jonka kertaluku on muotoa $2p$ ja joka ei ole syklinen. Osoitetaan, että tällöin välttämättä $G'$ on isomorfinen yllä esitetyn ryhmän $G$ kanssa. Ryhmällä $G'$ on aliryhmä $K' = \langle a' \rangle$, jonka kertaluku on $p$ ja alkio $b'$, jonka kertaluku on 2 siten että

$$G' = \{1, a', (a')^2, \ldots, (a')^{p-1}, b', b'a', b'(a')^2, \ldots, b'(a')^{p-1}\},$$

missä $i \in \{0, 1, \ldots p-1\}$. Lisäksi tälle ryhmälle pätee

$$(b'(a')^i)^2 = e \text{ ja } b'(a')^i = (a')^{p-1}b'.$$

Koska aliryhmässä $K'$ on $p$ alkiota ja sen sivuluokassa $b'K'$ ($b' \notin K'$) täytyy olla saman verran alkioita ja nämä sivuluokat ovat erillisiä, niin $G' = K' \cup b'K'$. Kaikki yllä esitetyt alkiot ovat tällöin erillisiä. Määritellään kuvaus $f : G \to G'$ siten että

$$f : b^j a^i \mapsto (b')^j (a')^i,\ j \in \{0, 1\}, i \in \{0, 1, \ldots, p-1\}.$$

Osoitetaan, että tämä kuvaus on isomorfismi. Koska alkiot $b^j a^i \in G$ ja $(b')^j (a')^i$ ovat kaikki erillisiä, kun $j \in \{0, 1\}$ ja $i \in \{0, 1, \ldots, p-1\}$, niin kuvaus on hyvin määritelty. Kuvaus on selvästi surjektio, sillä kaikille $(b')^j (a')^i \in G'$ löytyy $b^j a^i \in G$ niin että $f(b^j a^i) = (b')^j (a')^i$. Koska ryhmässä $G$ ja $G'$ on yhtä monta alkiota ja $f : G \to G'$ on surjektio, niin kaikki alkiot kuvautuvat eri alkioille eli $f$ on injektio ja siten myös bijektio,

Osoitetaan, että kuvaus $f$ on myös homomorfismi. Olkoot $g_1, g_2 \in G$, joten $g_1 = b^j a^i$ ja $g_2 = b^s a^t$ joillakin $j, s \in \{0, 1\}$ ja $i, t \in \{0, 1, \ldots, p-1\}$. Käytetään hyväksi seuraavia aiemmin saatuja yhtälöitä

$$(ba^i)^2 = e, ba^i = a^{p-i}b \text{ ja } (b'(a')^i)^2 = e, b'(a')^i = (a')^{p-i}b.'$$

Olkoon ensiksi $s = 0$, jolloin saadaan

$$f(g_1 g_2) = f((b^j a^i)(a^t)) = f(b^j a^{i+t}) = (b')^j (a')^{i+t} = (b')^j (a')^i (a')^t = f(b^j a^i) f(a^t) = f(g_1) f(g_2).$$

Olkoon seuraavaksi $s = 1$, jolloin

$$\begin{aligned} f(g_1 g_2) &= f((b^j a^i)(ba^t)) = f(b^j b a^{p-i} a^t) = f(b^{j+1} a^{p-i+t}) = (b')^{j+1} (a')^{p-i+t} \\ &= (b')^j b' (a')^{p-i} (a')^t = (b')^j b' (a')^{p-i} (b')^2 (a')^t = (b')^j b' b' (a')^i b' (a')^t \\ &= (b')^j (b')^2 (a')^i b' (a')^t = (b')^j (a')^i b' (a')^t = f(b^j a^i) f(ba^t) = f(g_1) f(g_2), \end{aligned}$$

joten kuvaus $f$ on homomorfismi tapauksissa $s = 0$ ja $s = 1$. On siis osoitettu, että kaikki ei-sykliset ryhmät, jotka ovat kertalukua $2p$, ovat isomorfisia keskenään, kun $p$ on

alkuluku ja $p \neq 2$. Tämän ei-syklisen ryhmän lisäksi on olemassa syklinen ryhmä, joka on kertalukua $2p$.

On siis olemassa korkeintaan kaksi kertalukua $2p$ olevaa ryhmää, jotka eivät ole isomorfisia keskenään. Tämä ei kuitenkaan vielä tarkoita, että jokaisella alkuluvulla $p$ nämä ryhmät löytyisivät. On selvää, että jokaiselle $n \in \mathbb{N}$ on olemassa syklinen ryhmä, joka on kertalukua $n$, joten kertalukua $2p$ oleva syklinen ryhmä löytyy varmasti. Kappaleessa 5 esittelin diedriryhmät ja totesin, että jokaiselle $n \in \mathbb{N}$ löytyy diedriryhmä $D_n$, jonka kertaluku on $2n$ ja joka ei ole syklinen. Nyt olemme löytäneet kaikki kertalukua $2p$ olevat ryhmät. Tässä tapauksessa oltiin kiinnostuneita ryhmistä, joiden kertaluvut ovat 6, 10 ja 14. Kertalukua 6 olevat ryhmät ovat $\mathbb{Z}_6$ ja $D_3$, kertalukua 10 olevat ryhmät $\mathbb{Z}_{10}$ ja $D_5$ ja kertalukua 14 olevat ryhmät $\mathbb{Z}_{14}$ ja $D_7$.

# Luku 9

# Kertaluku 8

Tutkitaan ensin kertalukua 8 olevia Abelin ryhmiä. Luvun 8 tekijät ovat 1, 2, 4 ja 8, joten lauseen 2.17 perusteella saadaan, että mahdolliset ryhmät ovat $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ja $\mathbb{Z}_2 \times \mathbb{Z}_4$. Seuraavaksi tulee vielä osoittaa, että nämä ryhmät eivät ole isomorfisia keskenään. Ryhmä $\mathbb{Z}_8$ on selvästi syklinen, sillä se on alkionsa $[1]_8$ virittämä. Tutkitaan ryhmän $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ alkoiden kertalukuja.

$$
\begin{aligned}
1([0]_8, [0]_8, [0]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([0]_8, [0]_8, [1]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([0]_8, [1]_8, [0]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([1]_8, [0]_8, [0]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([0]_8, [1]_8, [1]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([1]_8, [1]_8, [0]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([1]_8, [0]_8, [1]_8) &= ([0]_8, [0]_8, [0]_8) \\
2([1]_8, [1]_8, [1]_8) &= ([0]_8, [0]_8, [0]_8)
\end{aligned}
$$

Havaitaan, että tässä ryhmässä kaikkien alkioiden, neutraalialkiota lukuunottamatta, kertaluku on kaksi, joten se ei voi olla isomorfinen ryhmän $\mathbb{Z}_8$ kanssa. Tarkastellaan vielä ryhmän $\mathbb{Z}_2 \times \mathbb{Z}_4$ alkioiden monikertoja.

$$
\begin{aligned}
1([0]_2,[0]_4) &= ([0]_2,[0]_4)\\
4([0]_2,[1]_4) &= ([0]_2,[0]_4)\\
2([0]_2,[2]_4) &= ([0]_2,[0]_4)\\
2([0]_2,[3]_4) &= ([0]_2,[0]_4)\\
2([1]_2,[0]_4) &= ([0]_2,[0]_4)\\
4([1]_2,[1]_4) &= ([0]_2,[0]_4)\\
4([1]_2,[2]_4) &= ([0]_2,[0]_4)\\
4([1]_2,[3]_4) &= ([0]_2,[0]_4)
\end{aligned}
$$

Tämä ryhmä ei siis ole syklinen, joten $\mathbb{Z}_2 \times \mathbb{Z}_4 \ncong \mathbb{Z}_8$. Lisäksi voidaan havaita helposti, että esimerkiksi alkion $([0]_2,[1]_4)$ kertaluku on neljä, joten ryhmä $\mathbb{Z}_2 \times \mathbb{Z}_4$ ei myöskään voi olla isomorfinen ryhmän $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ kanssa. Näin on onnistuttu löytämään kolme Abelin ryhmää, joiden kertaluku on kahdeksan: $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ja $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Olkoon nyt $G$ kertalukua kahdeksan oleva ei-Abelin ryhmä. Tällöin $G$ ei siis ole myöskään syklinen eli jos $a \in G$, niin ei voi päteä, että $|a| = 8$. Lagrangen lauseen mukaan ryhmän alkion kertaluvun on jaettava koko ryhmän kertaluku eli jos $a \neq e$, niin $|a| = 2$ tai $|a| = 4$. Jos ryhmän $G$ jokaisen alkion kertaluku on kaksi (neutraalialkiota lukuunottamatta) ja jos $a, b \in G$, niin $(ab)^2 = e$ eli $abab = e$. Koska $a^2 = b^2 = e$, niin pätee $ba = a^2bab^2 = a(ab)^2b = ab$, mikä on ristiriidassa sen kanssa, että $G$ ei ole Abelin ryhmä. Ryhmässä $G$ täytyy siis olla alkio, jonka kertaluku on neljä. Olkoon $\langle a \rangle$ ryhmän $G$ aliryhmä ja $|\langle a \rangle| = 4$. Jos $b \in G$, mutta $b \notin \langle a \rangle$, niin sivuluokat $\langle a \rangle = \{e, a, a^2, a^3\}$ ja $b\langle a \rangle = \{b, ba, ba^2, ba^3\}$ sisältävät kaikki ryhmän G alkiot. Jos näin ei olisi, niin pätisi, että $ba^m = a^n$ joillakin $m, n \in \{1, 2, 3\}$, mistä seuraisi, että $b = a^n a^{-m}$. Koska $a^n, a^{-m} \in \langle a \rangle$, niin tällöin myös pätisi $b \in \langle a \rangle$, mikä on ristiriidassa oletuksen kanssa. Alkiot $a$ ja $b$ virittävät ryhmän $G$ ja alkiolle $a$ pätee $a^4 = e$. Kaikki ryhmän $G$ alkiot ovat siis esitettävissä sen alkioiden $a$ ja $b$ avulla, joten $G = \langle a, b \rangle$ ja lisäksi pätee $a^4 = e$. Koska sivuluokkia on vain kaksi, niin lauseen 2.26 perusteella $\langle a \rangle$ on normaali ja $G/\langle a \rangle = \{\langle a \rangle, b\langle a \rangle\}$ on isomorfinen ryhmän $\mathbb{Z}_2$ kanssa. Osoitetaan $b^2 \in \langle a \rangle$ vastaoletuksen avulla. Jos $b^2 \notin \langle a \rangle$, niin $b^2 \in b\langle a \rangle$. Tutkitaan, mikä sivuluokan $b\langle a \rangle$ alkioista $b^2$ tällöin olisi.

$$
\begin{aligned}
b^2 = b &\Rightarrow b = 1 \in \langle a \rangle\\
b^2 = ba &\Rightarrow b = a \in \langle a \rangle\\
b^2 = ba^2 &\Rightarrow b = a^2 \in \langle a \rangle\\
b^2 = ba^3 &\Rightarrow b = a^3 \in \langle a \rangle
\end{aligned}
$$

Koska oletettiin, että $b \notin \langle a \rangle$ ja jokaisessa tapauksessa päädyttiin ristiriitaan tämän kanssa, niin täytyy päteä, että $b^2$ on jokin sivuluokan $\langle a \rangle$ alkioista. Jos $b^2 = a$, niin $b^8 = e$.

Tutkitaan, mikä olisi tällöin alkion $b$ kertaluku. Jos $|b| = 2$, niin $a = e$, mikä on ristiriita. Jos puolestaan $|b| = 4$, niin $a^2 = e$ ja päädyttäisiin jälleen ristiriitaan. Alkion $b$ kertaluvun täytyy siis olla 8. Mutta tällöin $G = \langle b \rangle$ ja $G$ olisi syklinen ja siten myös Abelin ryhmä, mikä olisi ristiriidassa alkuperäisen oletuksen kanssa, joten $b^2 \neq a$. Jos puolestaan $b^2 = a^3$ ja $|b| = 2$, niin pätisi $a^3 = e$ ja jos $|b| = 4$, niin $a^2 = e$, joten ainoaksi vaihtoehdoksi jäisi $|b| = 8$. Edellä esitetyin perusteluin tämä olisi ristiriidassa sen kanssa, että oletimme ryhmän $G$ olevan epävaihdannainen, joten $b^2 \neq a^3$. Ainoiksi mahdollisiksi vaihtoehdoiksi jäävät $b^2 = e$ tai $b^2 = a^2$.

Koska $\langle a \rangle$ on ryhmän $G$ normaali aliryhmä, niin $b\langle a \rangle = \langle a \rangle b$ kaikilla $b \in G$. Tästä seuraa suoraan, että $b\langle a \rangle b^{-1} = \langle a \rangle$, joten $\langle a \rangle$ on isomorfinen ryhmän $b\langle a \rangle b^{-1}$ kanssa ja $bab^{-1} \in \langle a \rangle$. Näytetään seuraavaksi, että alkion $bab^{-1}$ täytyy olla kertalukua 4. Tehdään vastaoletus, että $|bab^{-1}| \neq 4$. Koska alkion kertaluvun täytyy jakaa ryhmän kertaluku, niin mahdolliset vaihtoehdot ovat, että $|bab^{-1}| = 1$ tai $|bab^{-1}| = 2$. Jos kertaluku on 1, niin $bab^{-1} = e$ ja $a = e$, mikä on ristiriita. Jos puolestaan kertaluku on 2, niin

$$\begin{aligned} & (bab^{-1})(bab^{-1}) = e \\ \Rightarrow\ & baab^{-1} = e \\ \Rightarrow\ & ba^2b = e \\ \Rightarrow\ & ba^2 = b \\ \Rightarrow\ & a^2 = e \end{aligned}$$

Jälleen päädytään ristiriitaan, joten $|bab^{-1}| = 4$. Sivuluokan $\langle a \rangle$ alkioista vain $a$ ja $a^3$ ovat kertalukua 4. Jos $bab^{-1} = a$, niin $ba = ab$ ja $G$ on Abelin ryhmä, mikä on vastoin oletustamme. Siispä $bab^{-1} = a^3$ eli toisin sanoen $ba = a^3b$. Näin saadaan kaksi mahdollisuutta ryhmälle $G$:

$$G_1 = \langle a, b \rangle \ \text{ ja } \ a^4 = 1, b^2 = a^2, ba = a^3b \tag{9.1}$$

$$G_2 = \langle a, b \rangle \ \text{ ja } \ a^4 = 1, b^2 = 1, ba = a^3b. \tag{9.2}$$

Olkoon $Q_8$ matriisien kertolaskulla varustettu ryhmä, jonka virittävät alkiot

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

ja

$$B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

missä $i^2 = -1$. Osoitetaan, että kyseessä on ei-Abelin ryhmä ja sen kertaluku on kahdeksan. Tutkitaan ensin millaisia alkioita voidaan muodostaa laskemalla yhteen alkioita $A$ ja $B$ sekä niiden monikertoja.

$$A^0B^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$A^0B^1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$A^0B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$A^0B^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

$$A^1B^0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$A^1B^1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$A^1B^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$A^1B^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

Vaikuttaisi siltä, että ryhmän $Q_8$ alkiot voidaan esittää muodossa $A^iB^j$, missä $i \in \{0,1\}$ ja $j \in \{0,1,2,3\}$. Osoitetaan, että näin tosiaankin pätee. Huomataan, että

$$BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = A^3B,$$

joten kaikki ryhmän $Q_8$ alkiot voidaan esittää muodossa $A^iB^j$. On helposti huomattavissa, että $A^4 = I$ ja $B^4 = I$, joten $i$ ja $j$ ovat positiivisia kokonaislukuja. Matriiseja pyörittelemällä saadaan selville myös, että $A^2 = B^2$ ja toisaalta $A^4 = e = A^0$. Lisäksi pätee seuraavaa:

$$\begin{aligned} & A^3B = BA \\ \Rightarrow\ & A^3 = BAB^{-1} \\ \Rightarrow\ & A^3 = BAB^3 \\ \Rightarrow\ & A^3 = AB^3B^3 \\ \Rightarrow\ & A^3 = AB^6 \\ \Rightarrow\ & A^3 = AB^2. \end{aligned}$$

Nyt siis jokainen ryhmän $Q_8$ alkio voidaan esittää muodossa $A^iB^j$, missä $i \in \{0,1\}$ ja $j \in \{0,1,2,3\}$. Erilaisia kombinaatioita on näin ollen kahdeksan, joten ryhmässä $Q_8$ on korkeintaan kahdeksan alkiota. Toisaalta aiemmin löydettiin kahdeksan erillistä alkiota kertomalla alkioita $A$ ja $B$ sekä niiden monikertoja, joten $Q_8$ koostuu täsmälleen näistä alkioista ja voidaan määritellä $Q_8 = \langle A, B \rangle$, missä $A^4 = 1, B^2 = A^2$ ja $BA = A^3B$. Ryhmä $Q_8$ on siis isomorfinen aiemmin määritellyn ryhmän $G_1$ kanssa. Tätä ryhmää kutsutaan nimellä *kvaterniooryhmä*.

Osoitetaan seuraavaksi, että *neliön symmetriaryhmä* $D_4$, jonka virittävät alkiot

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

ja

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

on isomorfinen ryhmän $G_2$ kanssa. Lasketaan jälleen mahdollisia alkioita.

$$A^0B^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^1B^0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$A^2B^0 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$A^3B^0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$A^0B^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$A^1B^1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$A^2B^1 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

$$A^3B^1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Tällä kertaa huomataan, että alkion $A$ kertaluku on 4 ja alkion $B$ kertaluku on 2. Laskemalla matriisien avulla saadaan $BA = A^3B$. Ryhmän $D_4$ alkiot voidaan siis ilmaista

muodossa $A^iB^j$. Koska $B^2 = e$, niin $B^3 = BB^2 = B$, joten $i \in \{0,1,2,3\}$ ja $j \in \{0,1\}$. Jälleen tämän perusteella erillisiä alkioita on korkeintaan kahdeksan. Nämä alkiot löydettiin yllä, joten pätee $D_4 = \langle A, B\rangle$, missä $A^4 = 1, B^2 = 1, BA = A^3B$ ja $D_4 \cong G_2$. Seuraavassa taulukossa on laskettu ryhmien $Q_8$ ja $D_4$ alkioiden kertaluvut.

| $Q_8$ | Kertaluku | $D_4$ | Kertaluku |
|---|---|---|---|
| $A^0B^0$ | 1 | $A^0B^0$ | 1 |
| $A^0B$ | 4 | $AB^0$ | 4 |
| $A^0B^2$ | 2 | $A^2B^0$ | 2 |
| $A^0B^3$ | 4 | $A^3B^0$ | 4 |
| $AB^0$ | 4 | $A^0B$ | 2 |
| $AB$ | 4 | $AB$ | 2 |
| $AB^2$ | 4 | $A^2B$ | 2 |
| $AB^3$ | 4 | $A^3B$ | 2 |

Koska ryhmässä $Q_8$ on 6 alkiota, joiden kertaluku on 4 ja ryhmässä $D_4$ ainoastaan 2 tällaista alkiota, niin ryhmät $Q_8$ ja $D_4$ eivät ole isomorfisia. Kertalukua 8 olevia ryhmiä ovat siis Abelin ryhmät $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4$ ja $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ sekä epävaihdannaiset ryhmät $Q_8$ ja $D_4$.

# Luku 10

# Kertaluku 12

Luku 12 voidaan jakaa epätriviaaleihin tekijöihin seuraavasti:

$$12 = 2 \cdot 6$$
$$12 = 2 \cdot 2 \cdot 3$$
$$12 = 3 \cdot 4.$$

Koska $2 \nmid 3$ ja $3 \nmid 4$, niin lauseen 2.17 perusteella ainoat vaihtoehdot Abelin ryhmiksi ovat $\mathbb{Z}_{12}$ ja $\mathbb{Z}_2 \times \mathbb{Z}_6$. Tutkitaan ryhmän $\mathbb{Z}_2 \times \mathbb{Z}_6$ alkioiden monikertoja.

$$1 \cdot ([0]_2, [0]_6) = e$$
$$6 \cdot ([0]_2, [1]_6) = e$$
$$3 \cdot ([0]_2, [2]_6) = e$$
$$2 \cdot ([0]_2, [3]_6) = e$$
$$3 \cdot ([0]_2, [4]_6) = e$$
$$6 \cdot ([0]_2, [5]_6) = e$$
$$2 \cdot ([1]_2, [0]_6) = e$$
$$6 \cdot ([1]_2, [1]_6) = e$$
$$6 \cdot ([1]_2, [2]_6) = e$$
$$2 \cdot ([1]_2, [3]_6) = e$$
$$6 \cdot ([1]_2, [4]_6) = e$$
$$6 \cdot ([1]_2, [5]_6) = e$$

Huomataan, että ryhmästä $\mathbb{Z}_2 \times \mathbb{Z}_6$ ei löydy alkiota, jonka kertaluku olisi 12, joten se ei voi olla isomorfinen syklisen ryhmän $\mathbb{Z}_{12}$ kanssa.

Esitellään ensiksi kertalukua 12 olevat ryhmät $D_6, A_4$ ja $T$, ja näytetään, että ne eivät ole isomorfisia keskenään. Osoitetaan lopuksi, että ne ovat itse asiassa ainoat kertalukua 12 olevat ei-Abelin ryhmät.

Olkoon $T$ määritelty niin, että sen virittävät alkiot $a$ ja $b$, joille pätee $|a| = 6$, $b^2 = a^3$ ja $ba = a^{-1}b$. Osoitetaan, että kyseessä on ryhmän $S_3 \times \mathbb{Z}_4$ aliryhmä, joka ei ole vaihdannainen ja jonka kertaluku on 12. Esimerkin 2.4 perusteella $S_3 \times \mathbb{Z}_4$ tosiaan on ryhmä. Merkitään ryhmän $S_3 = \{(1), (12), (23), (13), (123), (132)\}$ alkioita seuraavasti:

$$\begin{aligned} 1 &= (1) \\ \delta_1 &= (12) \\ \delta_2 &= (23) \\ \delta_3 &= (13) \\ \rho_1 &= (123) \\ \rho_2 &= (132). \end{aligned}$$

Tutkitaan ensiksi alkioiden $a = (\rho_1, [2]_4)$ ja $b = (\delta_1, [1]_4)$ monikertoja ja osoitetaan, että ne toteuttavat edellä esitetyt ehdot ja virittävät ryhmän $T$.

$$\begin{aligned} a^0b^0 &= (1, [0]_4) = e \\ ab^0 &= (\rho_1, [2]_4) \\ a^2b^0 &= (\rho_2, [0]_4) \\ a^3b^0 &= (1, [2]_4) \\ a^4b^0 &= (\rho_1, [0]_4) \\ a^5b^0 &= (\rho_2, [2]_4) \\ a^0b &= (\delta_1, [1]_4) \\ ab &= (\delta_3, [3]_4) \\ a^2b &= (\delta_2, [1]_4) \\ a^3b &= (\delta_1, [3]_4) \\ a^4b &= (\delta_3, [1]_4) \\ a^5b &= (\delta_2, [3]_4). \end{aligned}$$

Huomataan, että $|a| = 6$ ja $a^3 = (1, [2]_4) = b^2$. Lisäksi

$$ba = (\delta_1, [1]_4)(\rho_1, [2]_4) = (\delta_2, [3]_4) = a^5b = a^{-1}b,$$

joten alkiot $a = (\rho_1, [2]_4)$ ja $b = (\delta_1, [1]_4)$ toteuttavat ehdot ja virittävät ryhmän $T$. Koska $ba = a^{-1}b$, niin kaikki tämän ryhmän alkiot voidaan järjestää muotoon $a^ib^j$. Tarkastellaan

mitä arvoja eksponentit $i$ ja $j$ voivat olla. Ensinnäkin riittää tutkia positiivisia kokonaislukuja. Koska $|a| = 6$, niin $i \in \{0, 1, \dots 5\}$. Tarkastellaan alkion $b$ potensseja:

$$b^2 = a^3$$

$$b^3 = b^2 b = a^3 b$$
$$b^4 = b^2 b^2 = a^3 a^3 = a^6 = e.$$

Riittää siis, että $j \in \{0, 1\}$ eli ryhmän $T$ alkiot voidaan esittää muodossa $a^i b^j$, missä $i \in \{0, 1, \dots 5\}$ ja $j \in \{0, 1\}$. Erilaisia kombinaatioita on 12 kappaletta. Toisaalta edellä löysimme jo 12 erillistä alkiota, joten $|T| = 12$.

Osoitetaan, että $T$ on ryhmän $S_3 \times \mathbb{Z}_4$ aliryhmä käymällä läpi määritelmän 2.2 ehdot (H1)–(H3):

**(H1)** Joukko $H$ on suljettu laskutoimituksen suhteen, sillä jos $g_1, g_2 \in T$, niin $g_1 = a^i b^j$ ja $g_2 = a^s a^t$ joillakin $i, s \in \{0, 1, \dots 5\}$ ja $j, t \in \{0, 1\}$, jolloin $g_1 g_2 = a^i b^j a^s a^t$ voidaan järjestellä niin, että se on muotoa $a^m b^n$ joillakin $m \in \{0, 1, \dots, 5\}, n \in \{0, 1\}$ eli $g_1 g_2 \in T$.

**(H2)** Ryhmän $S_3 \times \mathbb{Z}_4$ neutraalialkio $(1, [0]_4)$ on joukossa $T$.

**(H3)** Näytetään, että joukko $T$ sisältää kaikkien alkioidensa käänteisalkiot:

$$(1, [0]_4)(1, [0]_4) = e$$

$$(1, [2]_4)(1, [2]_4) = e$$
$$(\rho_1, [2]_4)(\rho_2, [2]_4) = (\rho_2, [2]_4)(\rho_1, [2]_4) = e$$
$$(\rho_2, [0]_4)(\rho_1, [0]_4) = (\rho_1, [0]_4)(\rho_2, [0]_4) = e$$
$$(\delta_1, [3]_4)(\delta_1, [1]_4) = (\delta_1, [1]_4)(\delta_1, [3]_4) = e$$
$$(\delta_3, [3]_4)(\delta_3, [1]_4) = (\delta_3, [1]_4)(\delta_3, [3]_4) = e$$
$$(\delta_2, [3]_4)(\delta_2, [1]_4) = (\delta_2, [1]_4)(\delta_2, [3]_4) = e.$$

Lisäksi tämä ryhmä ei ole vaihdannainen, sillä $ba = a^{-1}b = a^5 b \neq ab$.

Tutkitaan seuraavaksi alternoivaa ryhmää $A_4$. Alternoivalla ryhmällä $A_n$ tarkoitetaan ryhmän $S_n$ parillisten permutaatioiden joukkoa. Osoitetaan ensin, että $A_n$ on symmetrisen ryhmän $S_n$ aliryhmä.

**(H1)** Olkoot $\sigma, \tau \in A_n$, jolloin molemmat ovat määritelmän mukaan parillisen määrän vaihtoja tuloja eli

$$\sigma = \sigma_1 \cdots \sigma_r \quad \text{ja} \quad \tau = \tau_1 \cdots \tau_s,$$

jossa $\sigma_1, \ldots, \sigma_r$ ja $\tau_1, \ldots, \tau_s$ ovat vaihtoja ja $r$ ja $s$ ovat parillisia. Tällöin

$$\sigma\tau = \sigma_1 \cdots \sigma_r \cdot \tau_1 \cdots \tau_s,$$

eli tulo $\sigma\tau$ on parillisen monen vaihdon tulo, joten $\sigma\tau \in A_n$.

**(H2)** Neutraalialkio (1) on määritelmänsä mukaan parillinen permutaatio, joten $(1) \in A_n$.

**(H3)** Osoitetaan vielä, että alkion $\sigma$ käänteisalkio on parillinen permutaatio. Koska

$$\sigma^{-1} = \sigma_r^{-1} \cdots \sigma_1^{-1} = \sigma_r \cdots \sigma_1,$$

niin myös $\sigma^{-1}$ on parillisen monen vaihdon tulo ja $\sigma^{-1} \in A_n$.

Erityisesti siis

$$A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

on symmetrisen ryhmän $S_4$ aliryhmä. Selvästikään ryhmä $A_4$ ei ole vaihdannainen, sillä esimerkiksi $(123)(124) = (13)(24)$ mutta $(124)(123) = (14)(23)$.

Kolmas kertalukua 12 oleva ei-Abelin ryhmä on diedriryhmä $D_6$ (kts. kappale 5), jonka virittävät alkiot $a = (123456)$ ja $b = (26)(35)$. Tämä ryhmä koostuu seuraavista alkioista:

$$a^0b^0 = (1)$$
$$ab^0 = (123456)$$
$$a^2b^0 = (135)(246)$$
$$a^3b^0 = (14)(25)(36)$$
$$a^4b^0 = (153)(264)$$
$$a^5b^0 = (165432)$$
$$a^0b = (26)(35)$$
$$ab = (12)(36)(45)$$
$$a^2b = (13)(46)$$
$$a^3b^= (14)(23)(56)$$
$$a^4b = (15)(24)$$
$$a^5b = (16)(25)(34).$$

Seuraavassa taulukossa on esitetty ryhmien $T, A_4$ ja $D_6$ alkioiden kertalukuja.

| $T$ | Kertaluku | $A_4$ | Kertaluku | $D_6$ | Kertaluku |
|---|---|---|---|---|---|
| $((1), [0]_4)$ | 1 | $(1)$ | 1 | $(1)$ | 1 |
| $((123), [0]_4)$ | 3 | $(123)$ | 3 | $(123456)$ | 6 |
| $((123), [2]_4)$ | 6 | $(132)$ | 3 | $(135)(246)$ | 3 |
| $((1), [2]_4)$ | 2 | $(124)$ | 3 | $(14)(25)(36)$ | 2 |
| $((132), [0]_4)$ | 3 | $(142)$ | 3 | $(153)(264)$ | 3 |
| $((132), [2]_4)$ | 6 | $(134)$ | 3 | $(165432)$ | 6 |
| $((12), [1]_4)$ | 4 | $(143)$ | 3 | $(26)(35)$ | 2 |
| $((12), [3]_4)$ | 4 | $(234)$ | 3 | $(12)(36)(45)$ | 2 |
| $((23), [1]_4)$ | 4 | $(243)$ | 3 | $(13)(46)$ | 2 |
| $((23), [3]_4)$ | 4 | $(12)(34)$ | 2 | $(14)(23)(56)$ | 2 |
| $((13), [1]_4)$ | 4 | $(13)(24)$ | 2 | $(15)(24)$ | 2 |
| $((13), [3]_4)$ | 4 | $(14)(23)$ | 2 | $(16)(25)(34)$ | 2 |

Taulukkoa lukemalla havaitaan, että ryhmästä $T$ ja $D_6$ löytyy alkio, jonka kertaluku on 6, mutta ryhmässä $A_4$ kaikkien alkioiden kertaluku on korkeintaan 3, joten $A_4 \ncong T$ ja $A_4 \ncong D_6$. Ryhmästä $T$ löytyy lisäksi alkio, jonka kertaluku on 4 toisin kuin ryhmästä $D_6$, joten $T \ncong D_6$. Seuraavaksi halutaan vielä osoittaa, että nämä neljä algebran näkökulmasta eri ryhmää ovat ainoat kertalukua 12 olevat ei-Abelin ryhmät.

Olkoon $G$ ei-Abelin ryhmä, jonka kertaluku on 12. Lauseen 4.3 perusteella ryhmällä $G$ on Sylowin 3-aliryhmä $P$. Aliryhmän $P$ kertaluku on määritelmän mukaan $p^m$ jollakin $m \in \mathbb{N}$, mutta lauseen 3.1 mukaan aliryhmän kertaluvun on jaettava ryhmän kertaluku, jolloin $m = 1$ ja $|P| = 3$. Korollaarin 3.2 avulla saadaan, että

$$[G : P] = \frac{|G|}{|P|} = \frac{12}{3} = 4.$$

Lauseen 2.32 mukaan on olemassa homomorfismi $f : G \to S_4$, jonka ydin $K$ on aliryhmässä $P$. Koska lauseesta 2.22 seuraa, että $K \leq P$ ja toisaalta tiedetään, että aliryhmän kertaluku jakaa ryhmän kertaluvun, niin $K = P$ tai $K = \{e\}$. Jos $K = \{e\}$, niin lauseen 2.14 perusteella kuvaus $f$ on injektio. Tällöin kaikki ryhmän $G$ alkiot kuvautuvat eri alkioille eli $|\mathrm{Im} f| = 12$. Toisaalta lauseen 2.13 todistuksessa osoitettiin, että ryhmähomomorfismin kuvajoukko on maalijoukon aliryhmä. Ryhmä $G$ on tällöin isomorfinen ryhmän $S_4$ kertalukua 12 olevan aliryhmän kanssa.

Osoitetaan seuraavaksi, että alternoiva ryhmä $A_4$ on ainoa tällainen ryhmä. Olkoon $H$ ryhmän $S_4$ aliryhmä, jonka kertaluku on 12. Koska ryhmän $H$ indeksi on kaksi, niin lauseen 2.26 mukaan $H$ on normaali. Näytetään, että jokainen ryhmän $S_4$ kolmen sykli on myös aliryhmässä $H$. Koska $|H| = 12$, niin lauseen 4.1 perusteella ryhmässä $H$ on alkio, jonka kertaluku on 3. Toisin sanoen $H$ sisältää jonkin 3-syklin $(abc)$, missä $a, b, c \in \{1, 2, 3, 4\}$.

Osoitetaan, että tällöin mielivaltainen ryhmän $S_4$ 3-sykli $(rst)$, kun $r, s, t \in \{1, 2, 3, 4\}$, on myös aliryhmässä $H$. Koska $H$ on normaali aliryhmä, niin alkion $(abc)$ konjugaatit ovat myös ryhmässä $H$. Toisin sanoen alkiota $(abc)$ voidaan konjugoida ryhmän $S_4$ alkioilla, jolloin saatu alkio kuuluu aliryhmään $H$. Alkio $(ar)(bs)(ct)$ on selvästi ryhmässä $S_4$, jolloin

$$(ar)(bs)(ct)(abc)((ar)(bs)(ct))^{-1} = (ar)(bs)(ct)(abc)(ar)(bs)(ct) = (rst) \in H.$$

Koska mielivaltainen alkio $(rst)$ on aliryhmässä $H$, niin $H$ sisältää kaikki ryhmän $S_4$ 3-syklit.

Tarkastellaan seuraavaksi alternoivaa ryhmää $A_n$ ja näytetään, että $A_4 \cong H$. Olkoot $r, s \in \{1, 2, \ldots, n\}$. Osoitetaan, että tällöin ryhmän $A_n$ virittävät kolmen syklit $\{(rsk) \mid 1 \leq k \leq n, k \neq r, s\}$. Koska ryhmän $A_n$ muodostavat parilliset permutaatiot, niin voidaan ajatella, että $A_n$ koostuu muotoa $(ab)(cd)$ ja $(ab)(ac)$ olevien vaihtojen tuloista, kun $a, b, c, d \in \{1, 2, 3, 4\}$. (Riittää tutkia tällaista muotoa olevia vaihtoja, sillä esimerkiksi $(ab)(ab) = (1)$ ja $(aa)(bc) = (bc)$.) Koska $(ab)(cd) = (acb)(acd)$ ja $(ab)(ac) = (acb)$, niin ryhmä $A_n$ koostuu 3-sykleistä, jotka voivat olla muotoa

$$(rsa), (ras), (rab), (sab) \text{ tai } (abc),$$

missä $a, b$ ja $c$ ovat erillisiä ja $a, b, c \neq r, s$. Huomataan, että

$$(ras) = (rsa)^2$$

$$(rab) = (rsb)(ras) = (rsb)(rsa)^2$$

$$(sab) = (rbs)(rsa) = (rsb)^2(rsa)$$

$$(abc) = (ras)(rsc)(rbs)(rsa) = (rsa)^2(rsc)(rsb)^2(rsa),$$

joten ryhmän $A_n$ virittävät alkiot $\{(rsk) \mid 1 \leq k \leq n, k \neq r, s\}$. Näin ollen ryhmä $A_4$ on isomorfinen yllä esitetyn ryhmän $H$ kanssa ja ainoa ryhmän $S_4$ aliryhmistä, jonka indeksi on kaksi. Nyt on saatu osoitettua, että jos homomorfismin $f$ ydin $K$ sisältää vain neutraalialkion, niin ryhmä $G$ on isomorfinen alternoivan ryhmän $A_4$ kanssa.

Tutkitaan seuraavaksi tapausta $K = P$. Lauseen 2.22 mukaan homomorfismin $f : G \to S_4$ ydin on ryhmän $G$ normaali aliryhmä, joten $P \trianglelefteq G$. Koska $P$ on normaali ryhmässä $G$ ja tiedetään, että Sylowin 3-aliryhmät ovat konjugaatteja keskenään, niin $P$ on ainoa ryhmän $G$ aliryhmä, jonka kertaluku on 3. Tämä tarkoittaa, että ryhmässä $G$ on vain kaksi alkiota, joiden kertaluku on 3. Olkoon $c$ toinen näistä. Määritelmän mukaan alkion $c$ keskittäjä koostuu niistä ryhmän $G$ alkioista, jotka kommutoivat sen kanssa. Tällöin alkion $c$ konjugaattiluokka $[G : C_G(c)]$ koostuu joko ainoastaan alkiosta $c$ tai sen lisäksi toisesta alkiosta, joka on myös kertalukua 3. Nyt

$$[G : C_G(c)] = \frac{|G|}{|C_G(c)|},$$

joten $C_G(c)$ on ryhmä, jonka kertaluku on 12 tai 6. Lauseen 4.1 mukaan molemmissa tapauksissa ryhmässä $C_G(c)$ on alkio $d$, jonka kertaluku on 2. Koska $|c| = 3$ ja $|d| = 2$ ja lukujen 2 ja 3 pienin yhteinen monikerta on 6, niin $|cd| = 6$.

Olkoon $a = cd$. Koska $|\langle a \rangle| = 6$, niin $[G : \langle a \rangle] = 2$ ja lauseen 2.26 perusteella $\langle a \rangle$ on normaali aliryhmä. Lisäksi tiedetään, että $G/\langle a \rangle$ on ryhmä, jossa on kaksi alkiota. On siis olemassa alkio $b \in G$, jolle pätee $b \notin \langle a \rangle$ ja $b^2 \in \langle a \rangle$. Koska $\langle a \rangle$ on normaali, niin lauseen 2.21 mukaan $bab^{-1} \in \langle a \rangle$. Lauseen 2.30 todistuksessa osoitimme, että alkiolla $a$ on sama kertaluku kuin sen konjugaatilla, joten $|bab^{-1}| = 6$. Tutkitaan ryhmän $\langle a \rangle$ alkioiden monikertoja:

$$(a^2)^3 = a^6 = e \Rightarrow |a^2| \neq 6$$
$$(a^3)^2 = a^6 = e \Rightarrow |a^3| \neq 6$$
$$(a^4)^3 = a^12 = e \Rightarrow |a^4| \neq 6.$$

Alkio $bab^{-1}$ ei ole siis mikään alkioista $a^2, a^3$ tai $a^4$. Koska $G$ ei ole vaihdannainen ryhmä, niin $ab \neq ba$ eli $bab^{-1} \neg a$. Täytyy siis päteä, että $bab^{-1} = a^5$.

Tutkitaan seuraavaksi, mikä aliryhmän $\langle a \rangle$ alkioista $b^2$ on. Jos $b^2 = a^3$, niin yhtäpitävästi $b^3 = ba^2$. Toisaalta

$$ba^2 = b(aa) = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-1}(a^{-1}b) = (a^{-1}a^{-1})b = a^{-2}b = a^4b,$$

joten $b^3 = a^4b \Leftrightarrow b^2 = a^4$. Tällöin $a^2 = a^4$, mikä on yhtäpitävää sen kanssa, että $a^2 = e$, eli on päädytty ristiriitaan. Siispä $b^2 \neq a^2$ ja $b^2 \neq a^4$. Jos puolestaan $b^2 = a$, niin $b^{12} = e$, sillä alkion $a$ kertaluku on 6. Alkion $b$ kertaluvun tulee jakaa luku 12, joten vaihtoehdot kertaluvuksi ovat $2, 3, 4, 6$ ja 12. Tutkitaan nämä vaihtoehdot erikseen seuraavaksi:

$$|b| = 2 \Rightarrow a = e$$
$$|b| = 3 \Rightarrow e = b^6 = (b^2)^3 = a^3$$
$$|b| = 4 \Rightarrow e = b^4 = (b^2)^2 = a^2$$
$$|b| = 6 \Rightarrow e = b^6 = (b^2)^3 = a^3.$$

Nämä kaikki vaihtoehdot päätyvät ristiriitaan sen kanssa, että $|a| = 6$, jolloin alkion $b$ kertaluvun täytyy olla 12. Tällöin $b$ virittäisi koko ryhmän $G$, mutta oletimme, että $G$ ei ole Abelin ryhmä eli ei myöskään syklinen. Tällöin alkuperäinen väite, $b^2 = a$, on väärä. Täysin samanlaisella päättelyllä voidaan osoittaa, että $b^2 \neq a^5$. Näin ollen ainoat mahdollisuudet ryhmälle $G$ ovat seuraavat:

$$G_1 : |a| = 6, b^2 = e, ba = a^{-1}b \tag{10.1}$$
$$G_2 : |a| = 6, b^2 = a^3, ba = a^{-1}b. \tag{10.2}$$

Kappaleen 5 perusteella $G_1$ on isomorfinen ryhmän $D_6$ kanssa.

$G_2$ puolestaan on isomorfinen edellä esitetyn ryhmän $T$ kanssa, sillä aiemmin huomattiin, että ehdoista $|a| = 6, b^2 = a^3$ ja $ba = a^{-1}b$ seuraa, että kaikki tällaisen ryhmän alkiot voidaan esittää muodossa $a^i b^j$, missä $i \in \{0, 1, \ldots 5\}$ ja $j \in \{0, 1\}$. Erillisiä alkioita on siis korkeintaan 12 kappaletta ja nämä alkiot löydettiin tarkasteltaessa ryhmää $T$, joten $G_2 \cong T$.

# Luku 11

# Kertaluku 15

Näytetään, että kertalukua 15 olevia ryhmiä on vain yksi kappale, nimittäin syklinen ryhmä $\mathbb{Z}_{15}$. Olkoon $G$ ryhmä, jonka kertaluku on 15. Lauseen 4.3 perusteella ryhmällä $G$ on Sylowin 5-aliryhmä. Olkoon näitä Sylowin 5-aliryhmiä $s_5$ kappaletta, jolloin $s_5 \equiv 1 \pmod 5$ ja lisäksi $s_5$ jakaa luvun 3. Ainoa mahdollisuus on siis, että ryhmällä $G$ on vain yksi Sylowin 5-aliryhmä. Koska Sylowin 5-aliryhmät ovat konjugaatteja keskenään ja näitä aliryhmiä on vain yksi, niin sen täytyy olla normaali, eli $G$ ei ole yksinkertainen.

Tarkastellaan seuraavaksi ryhmän $G$ Sylowin 3-aliryhmiä. Olkoon niiden lukumäärä $s_3$, jolloin $s_3 \mid 5$ ja $s_3 \equiv 1 \pmod 3$. Sylowin 3-aliryhmiä on siis tässäkin tapauksessa vain yksi kappale ja tämäkin aliryhmä on normaali. Olkoon $H$ Sylowin 5-aliryhmä ja $K$ Sylowin 3-aliryhmä. Koska luvut 5 ja 3 ovat alkulukuja ja Lagrangen lauseen mukaan ryhmän jokaisen alkion kertaluvun on jaettava koko ryhmän kertaluku, niin aliryhmässä $H$ jokaisen alkion kertaluvun täytyy olla 5 ja aliryhmässä $K$ puolestaan 3 neutraalialkiota lukuunottamatta. Tällöin ryhmien $H$ ja $K$ leikkaus sisältää ainoastaan yhden alkion, nimittäin neutraalialkion. Osoitetaan seuraavaksi aliryhmäkriteeriä käyttäen, että $HK \leq G$. Ensinnäkin ryhmä $HK$ on epätyhjä, sillä se sisältää ryhmän $G$ neutraalialkion. Olkoot $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Koska ryhmä $K$ on normaali ja $k_1 k_2^{-1} \in K$, niin lauseen 2.21 perusteella $h_2(k_1 k_2^{-1})h_2^{-1} = k'$ jollakin $k' \in K$, mikä tarkoittaa, että $k_1 k_2^{-1} h_2^{-1} = h_2^{-1} k'$. Nyt

$$(h_1 k_1)(h_2 k_2)^{-1} = (h_1 k_1)(k_2^{-1} h_2^{-1}) = h_1(k_1 k_2^{-1} h_2^{-1}) = h_1 h_2^{-1} k' \in HK,$$

sillä $h_1 h_2^{-1} \in H$ ja $k' \in K$, joten $HK$ on ryhmän $G$ aliryhmä. Tämä aliryhmä sisältää ryhmät $H$ ja $K$ ja lisäksi sen kertaluvun täytyy jakaa luku 15, jolloin ainoa vaihtoehto on, että $HK = G$. Nyt lauseen 2.23 perusteella $G$ on isomorfinen ryhmän $H \times K$ kanssa ja siten myös $G \cong \mathbb{Z}_5 \times \mathbb{Z}_3$ kanssa. Ryhmä $G \cong \mathbb{Z}_5 \times \mathbb{Z}_3$ syklinen, sillä se on alkionsa $([1]_5, [1]_3)$ virittämä. Näin on saatu todistettua, että ainoa kertalukua 15 oleva ryhmä $G$ on Abelin ryhmä ja syklinen.

# Luku 12

# Kertaluvut 1–15

Tässä luvussa esittelen vielä taulukoituna kaikki kertalukua 1–15 olevat ryhmät, jotka olen tarkemmin esittänyt edellisissä luvuissa.

| Kertaluku | Ryhmät |
|---|---|
| 1 | $\mathbb{Z}_1$ |
| 2 | $\mathbb{Z}_2$ |
| 3 | $\mathbb{Z}_3$ |
| 4 | $\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$ |
| 5 | $\mathbb{Z}_5$ |
| 6 | $\mathbb{Z}_6,\ D_3$ |
| 7 | $\mathbb{Z}_7$ |
| 8 | $\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times Z_2,\ Q_8,\ D_4$ |
| 9 | $\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$ |
| 10 | $\mathbb{Z}_{10},\ D_5$ |
| 11 | $\mathbb{Z}_{11}$ |
| 12 | $\mathbb{Z}_{12},\ \mathbb{Z}_2 \times \mathbb{Z}_6,\ A_4,\ D_6,\ T$ |
| 13 | $\mathbb{Z}_{13}$ |
| 14 | $\mathbb{Z}_{14},\ D_7$ |
| 15 | $\mathbb{Z}_{15}$ |

# Kirjallisuutta

[1] B. Baumslag, B. Chandler, 1968: Theory and Problems of Group Theory. McGraw-Hill Book Company. Department of Mathematics New York University.

[2] J. Fraleigh, 1967: A First Course in Abstract Algebra. Addison-Wesley Publishing Company. Department of Mathematics University of Rhode Island.

[3] J.A. Gallian, 1986: Contemporary Abstract Algebra. D.C. Heath and Company, Lexington, Massachusetts, Toronto. University of Minnesota, Duluth.

[4] T. Hungerford, 1974: Algebra (Graduate Texts in Mathematics.) 3. painos. Springer-Verlag New York.

[5] J. Häsä, J. Rämö, 2012: Johdatus Abstraktiin Algebraan. Gaudeamus Helsinki.

[6] J. Häsä, 2010: Algebra II. Luentomateriaali. Helsingin yliopisto.